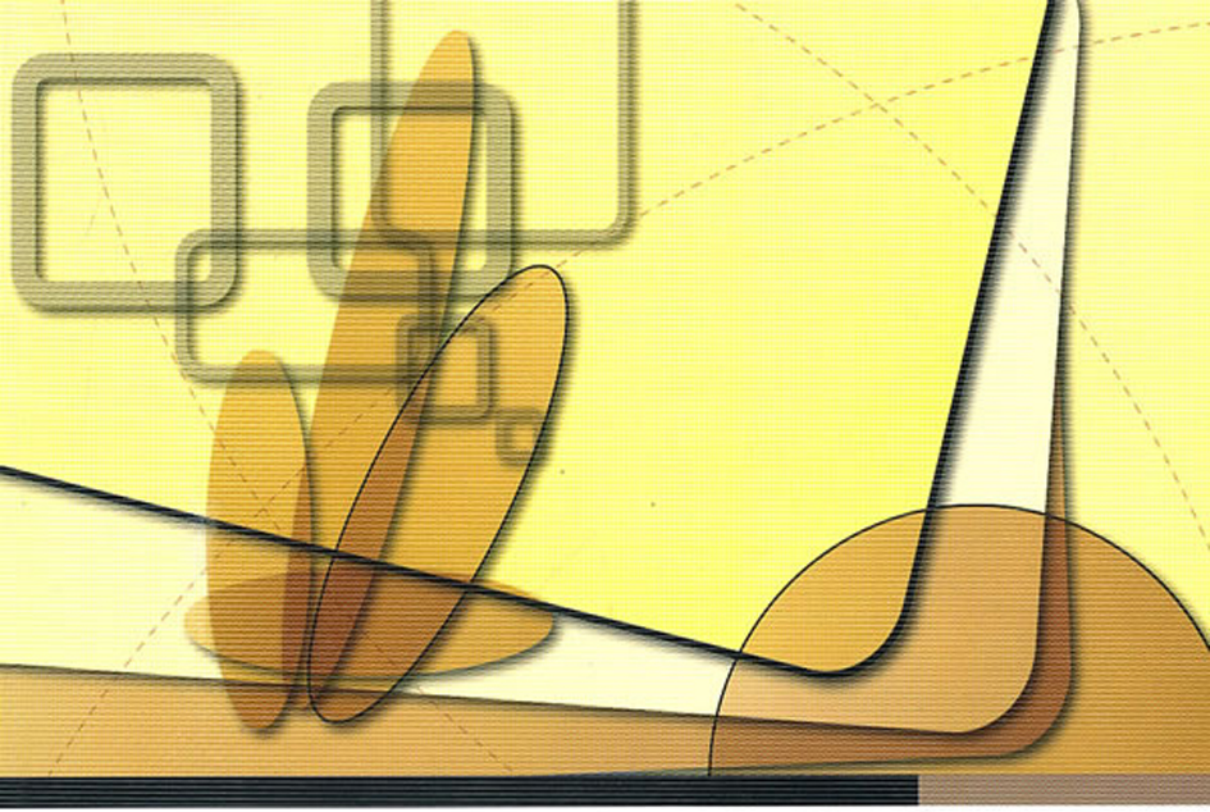


智能信息处理与应用

ZHINENG XINXI CHULI YU YINGYONG

李明　王燕　年福忠　编著

Intelligent
Information

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY

http://www.phei.com.cn

智能信息处理与应用

李　明　王燕　年福忠　编著

電子工業出版社

Publishing House of Electronics Industry

北京 • BEIJING

内 容 简 介

智能信息处理涉及信息学科的诸多领域。本书从理论方法和实践技术角度，论述了智能信息处理技术的主要概念、基本原理、典型方法及新的发展。本书共 11 章，包括不确定性信息处理、模糊集与粗糙集理论、人工神经网络、支持向量机、遗传算法、群体智能、人工免疫、量子算法、信息融合技术，以及智能信息处理技术在人脸识别和说话人识别中的应用。

本书适合从事智能信息处理研究的科研人员和智能系统开发与应用的工程技术人员阅读，也可作为研究生的相关课程或专题的参考书。

图书在版编目（CIP）数据

智能信息处理与应用 / 李明，王燕，年福忠编著. —北京：电子工业出版社，2010.9
ISBN 978-7-121-11798-5
I. ①智… Ⅱ. ①李… ②王… ③年… Ⅲ. ①人工智能－信息处理 Ⅳ. ①TP18

中国版本图书馆 CIP 数据核字（2008）第 176333 号

策划编辑：李 洁 （lijie@phei.com.cn）
责任编辑：侯丽平
印 刷：
装 订：
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编：100036
开 本：787×980 1/16 印张：18.25 字数：397 千字
印 次：2010 年 9 月第 1 次印刷
印 数：3 000 册 定价：39.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

智能信息处理涉及信息学科的诸多领域，是现代信号处理、人工神经网络、模糊系统理论、进化计算，以及人工智能等理论和方法的综合应用，它是计算机科学中的前沿交叉学科，也是应用导向的综合性学科。

“智能信息处理”的前身是以人工神经网络、进化计算和模糊系统为代表的“软计算”，它兴起于 20 世纪 90 年代后期。由于“软计算”方法可以有效地分析和处理不完备信息，因此它的理论日益受到国际学术界的重视，并且在模式识别、机器学习、决策支持、过程控制、故障诊断、预测建模等许多科学与工程领域得到了成功应用。进入 21 世纪后，人们逐渐用“智能信息处理”一词来表述“软计算”及其应用。

近年来，以人脸识别和说话人识别为代表的生物认证成了智能信息处理应用领域的一个研究热点。在各种利用人体生物特征进行身份识别的方法中，人脸识别以其直接、友好、方便的特点得到了越来越多的重视。同时，由于利用人脸来进行识别可以将其他方法无法获得的人物表情和心理特征考虑在内，也使人脸识别具有了其他识别方法无法比拟的有效性、适应性和灵活性。说话人识别技术是从语音波形中提取信息反应说话人的个性特征的，通过对语音个性特征参数的建模和识别，从而确定或鉴别说话人的身份。说话人识别具有不会被遗失和忘记、无须记忆、使用方便等特点。另外，由于语音信号采集方便，系统集成成本低，使说话人识别具有广泛的应用前景。无论是人脸识别还是说话人识别，其在经济、安全、社会保障、犯罪、军事等领域都有着巨大的潜在应用价值。

从 2005 年起，作者先后承担了多项相关的科研项目，对智能信息处理的一些理论和应用进行了研究和探索。我们的写作初衷就是结合自己的研究成果，反映出智能信息处理中的一些新方法、新应用。

全书共 11 章，包括不确定性信息处理、模糊集与粗糙集理论、人工神经网络、支持向量机、遗传算法、群体智能、人工免疫、量子算法、信息融合技术等当前智能信息处理领域内的一些经典理论和新方法，以及智能信息处理技术在人脸识别和说话人识别中的应用。

本书是作者多年来在从事该领域研究工作的基础上，参阅了国内外有关文献资料，结合作者的科研成果和学习心得，经过反复修改而成的。本书第 3、4、9、10、11 章由李明执笔，第 1、5、6、7、8 章由王燕执笔，第 2 章由年福忠执笔。张亚芬、郝元宏、邢玉娟、李伟娟、孙向风等研究生为本书的编写做出了许多贡献，对他们的工作表示感谢。

本书的出版，得到了兰州理工大学学术专著出版基金的资助，在此表示感谢！
由于作者水平所限，书中难免有不妥之处，欢迎读者不吝指正。

作　者

2010 年 3 月

目　　录

Chapter 1

第 1 章

不确定性信息处理

在日常生活和科学研究中，人们一直在追求用某一确定的数学模型来解决问题或描述现象。然而，真实世界是一个不断变化的、不完全的、不精确的，充满着矛盾的、复杂相关的信息世界。也就是说，用确定的概念描述事物往往是有局限性的。在现实世界中，包含有大量的柔性信息，表征出模糊性、复杂性和不精确性，因而对这些信息的处理就变得十分重要。

1.1 知识的不确定性[1]

知识的不确定性，首先反映在语言的不确定性上，因为语言是知识的载体。知识的不确定性，还反映在常识上，因为它通常是知识的知识，也称为元知识，是其他专业知识的基础。常识通常也是用自然语言表达的。语言中的基本单元是语言值，对应一个个概念，概念的不确定性有多个方面，主要有随机性和模糊性。

1.1.1 随机性

在自然界和人类社会中，经常会遇到这样一种现象：在完全相同的情况下，一个实验或观察（统称为实验）得到的结果可能是不同的。这种现象称为随机现象。其特点是：可重复观察，在观察之前知道所有可能的结果，但不知道到底哪一个结果会出现。这是一种由客观

条件决定的不确定现象。主要因为事件发生的条件不充分，使得条件与结果之间没有必然的因果关系，因而在事件的出现与否上表现出不确定性。

1.1.2 模糊性

不确定性的早期研究内容仅仅是针对随机性。随着研究的深入，人们发现有一类不确定现象无法用随机性来描述，这就是模糊性。

模糊性长期被排斥在科学殿堂之外。直到 20 世纪，人们才认识到，模糊性并不是坏事，相反倒是好事，它能够用较少的代价，传送足够的信息，并能对复杂事物做出高效率的判断和处理。也就是说，模糊性有助于提高效率。

1.1.3 自然语言中的不确定性

随机性和模糊性是不确定性最基本的两个方面。自然语言的不确定性是不确定性的另一个重要研究内容。

不确定性是客观世界固有的属性，自然语言作为客观世界的表述手段，人类思维的载体，就必然会具有不确定性。另外，单个人脑认知的局限性，也使得人对客观世界的描述会出现不确定性，这一点也会通过语言反映出来。对同一事件，不同人的认知能力的差异，也会表现在语言表述的差异上。因此，语言带有不确定性是很自然的，是人类思维的本质特征。

1.1.4 常识的不确定性

研究知识，必然要涉及常识，因为常识是任何人和任何专业都必须触及的。人的智能活动，包括判断、推理、抽象等都离不开常识。

在人们的日常生活中，“常识”意味着简单、通俗和普遍，似乎无须证明、司空见惯，习以为常。而与一般人的看法相反，在人工智能界，常识的表示、处理和验证恰恰是一个非常困难的问题。

常识至少应当具备普遍性和直接性。常识的普遍性和直接性，决定了它与专业知识不同，它不要求具备专业知识所必不可少的严密性、深刻性和系统性，而是具有很强的相对性，受时间、认识主体等多种元素的影响，是随着时间、地点、人群的不同而变化的。这是相对性带来的不确定性。

目前，人工智能界有这样的共识：有无常识是人和机器的根本区别之一。人的常识能否被物化，将决定人工智能最终能否实现。因此，常识和常识中的不确定性是无法避免的。

1.1.5　知识的其他不确定性

要把知识中的不确定性讲清楚是一件很困难的事情。但是随机性和模糊性是最基本的不确定性，它们反映在语言的不确定性或常识的不确定性之中。而在一个知识体系的框架中，还会有更高层次的不确定性，尤其是不完备性和不协调性。

知识的不完备性包括知识内容的不完整、知识结构的不完备等。内容的不完整，可能来源于获取知识时观测不充分、设备不精确，只获取了局部信息，因此对部分信息内容根本不知道；或者知道应该有某一个具体的信息值，但不清楚其大小。知识结构的不完备，可能因为人的认识能力、获取手段的限制等原因，造成对解决某个特定问题的背景和结构认识不全，忽略了一些重要因素。

不协调性是知识不确定性的另一种表现。知识的不协调是指知识内在的矛盾，不协调的程度可以依次为冗余、干扰、冲突等。冗余是指人们在解决问题时，存在某些重复的，多余知识的现象。干扰是指对当前待解决的问题不但没有帮助，反而会对其他知识起到阻碍、抑制的作用，甚至导致错误结果的现象。冲突即矛盾，指知识之间的相互抵触或完全对立。

不协调性是知识的不确定性的重要体现，人们不可能、也没有必要在一切场合下都试图消除知识的不协调性，要把不协调性看做是知识的一种常态，允许包容、折中和调和。

1.2　不确定性的度量方法[2]

在科学研究中，人们一直追求用确定的数学模型来描述现象和解决问题。为了解决知识的不确定性问题，也需要数学的支持，即需要采用某种数学方法来度量知识的不确定性。根据不确定性的特征，通常的度量方法有概率理论、模糊理论和粗糙集理论等。

1.2.1　概率度量和贝叶斯公式

不确定性与概率有许多内在的联系。因此，很早以来，研究人员就将概率理论引入人工智能中，它为研究知识的随机性奠定了数据基础，也为研究不确定性提供了工具。

1．事件的概率

在随机现象中，表示事件发生可能性大小的度量（数值）称为事件的概率。设 A 表示一个事件，则它的概率记做 $P(A)$。

概率具有如下一些性质。

（1）非负性：对于任一事件 A，有

$$0 \leqslant P(A) \leqslant 1 \tag{1.1}$$

（2）规范性：必然事件 D 的概率 $P(D)=1$，不可能事件 ϕ 的概率 $P(\phi)=0$。

性质（2）反过来不一定成立。就是说概率为 1 的事件不一定为必然事件。同样，概率为 0 的事件不一定为不可能事件。

（3）有限可加性：设事件 A_1，A_2，…，A_k 是两两互不相容的事件，即有 $A_i \cap A_j = \phi (i \neq j)$，则

$$P\left(\bigcup_{i=1}^{k} A_i\right) = \sum_{i=1}^{k} P(A_i) \tag{1.2}$$

即有限个互不相容的事件的和事件的概率等于这些事件的概率之和。

（4）对任一随机事件 A，有 $P(\overline{A}) = 1 - P(A)$。

（5）对任意两个事件 A、B，有 $P(A \cup B) = P(A) + P(B) - P(AB)$。

2．条件概率

设 A 和 B 是某个随机试验中的两个事件，如果在事件 B 发生的条件下考虑事件 A 发生的概率，就称它为事件 A 的条件概率，记做 $P(A|B)$，若 $P(B)>0$，则

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} \tag{1.3}$$

3．全概率公式与贝叶斯公式

（1）全概率公式

设事件 A_1，A_2，…，A_k 满足：

① 两两互不相容，即当 $i \neq j$ 时，$A_i \cap A_j = \phi$；

② $P(A_i) > 0$；

③ $D = \bigcup_{i=1}^{k} A_i$，$D$ 为必然事件。

则对任何事件 B 有下式成立：

$$P(B) = \sum_{i=1}^{k} P(A_i) P(B \mid A_i) \tag{1.4}$$

该公式称为全概率公式，它提供了一种计算 $P(B)$的方法。

（2）贝叶斯公式

设事件 A_1，A_2，…，A_k 满足上面的 3 个条件，则对任何事件 B 有下式成立：

$$P(A_i \mid B)=\frac{P(A_i)P(B \mid A_i)}{\sum_{j=1}^{k}P(A_j)P(B \mid A_j)} \qquad j=1,2,\cdots,k \tag{1.5}$$

上式称为贝叶斯公式。

1.2.2　模糊度量及性质

概率论是表示和处理随机性的强有力的工具。长期以来，人们认为不确定性就是随机性。后来，系统科学家 Zadeh 对此提出了挑战。他认为有一类不确定性问题无法用概率论去表示和度量，于是 1965 年他发表了 Fuzzy Sets[3]，并创立了模糊集合理论。

1．模糊性

所谓模糊性是指客观事物在性态及类属方面的不分明性，其根源是在类似事物间存在一系列过渡状态，它们相互渗透，相互贯通，使得彼此之间没有明显的界限。例如，我们通常说“某人很年轻”、“某人比较年轻”，但“很年轻”和“比较年轻”之间没有明确的界限，所以它们都是模糊的。

模糊性是客观世界中某些事物本身所具有的一种不确定性，它与随机性有着本质的区别。有明确定义但不一定出现的事件中包含的不确定性称为随机性，它不因人的主观意识变化，由事物本身的因果规律决定。而已经出现但难以给出精确定义的事件中包含的不确定性称为模糊性，是由事物的概念界限模糊和人的主观推理与判断产生的。

2．模糊集与隶属函数

设 U 是论域，μ_A 是把任意 $x\in U$ 映射为[0,1]上某个值的函数，即

$$\mu_A : U \to [0,1] \tag{1.6}$$

$$x \to \mu_A(x) \tag{1.7}$$

则 μ_A 为定义在 U 上的一个隶属函数，由 $\mu_A(x)(x\in U)$ 所构成的集合 A 称为 U 上的一个模糊集，$\mu_A(x)$ 称为 x 对 A 的隶属度。

3．模糊关系

设 $U_1, U_2, \cdots, U_n$ 是 n 个论域，$U_1\times U_2\times\cdots\times U_n$ 中的一个 n 元模糊关系 R 是 $U_1\times U_2\times\cdots\times U_n$ 上的一个模糊集，记为：

$$R=\int_{U_1\times U_2\times\cdots\times U_n}\mu_R(x_1,\cdots,x_n)/(x_1,\cdots,x_n) \tag{1.8}$$

模糊关系是经典集合论中关系的推广，一个有限论域上的二元模糊关系可以表示成隶属度矩阵的形式。

1.2.3 其他度量方法

模糊集理论使得区别于随机性的模糊性得到了一种数学的表述，从而不确定性的度量有了一套新的理论和方法。模糊集理论需要数据集合之外的先验信息，如要预先确定隶属度和隶属函数。一旦离开了隶属度和隶属函数，几乎所有的模糊集合运算都将难以进行。那么能否用不确定性本身提供的信息来研究和度量不确定性呢？20 世纪 80 年代，波兰科学家 Pawlak[4]基于边界区域的思想提出了粗糙集的概念，成为粗糙集理论的奠基人。

粗糙集理论把那些无法确认的个体都归属于边界线区域，而这些边界线区域被定义为上近似集和下近似集之差。由于它有确定的数学公式描述，所以含糊知识数目是可以计算的[5]。并且，根据粗糙集理论的思想，知识是有确定的粒度的，如果待研究知识的粒度和已知知识的粒度正好匹配，则待研究的知识是精确的，否则就在不精确的边界，即是粗糙的。

与概率论、模糊集合相比较，粗糙集理论从不可区分关系出发，以粒度为基础，研究知识的粗糙程度，丰富了不确定性的研究内容。

1.3 不确定性推理方法

不确定性推理是指知识不确定性的传播和更新，即新的不确定性知识的获取过程，是建立在不确定性知识和证据基础上的推理。例如，不完备、不精确知识的推理，模糊知识的推理等。实际上不确定性推理是一种从不确定的初始证据出发，通过运用不确定性知识，最终推出具有一定程度的不确定性但却又是合理或基本合理的结论的思维过程。不确定性推理的方法主要包括主观贝叶斯推理、模糊逻辑推理和证据理论[2,6,7]。

1.3.1 主观贝叶斯推理

主观贝叶斯方法是 R.O.Duda、P.E.Hart 等人 1976 年在贝叶斯公式的基础上经适当改进提出的。它是最早用于处理不确定性推理的方法之一，已在地矿勘探专家系统 PROSPECTOR 中得到了成功的应用。

1．基本概念

（1）几率函数：几率函数定义为

$$O(x)=\frac{P(x)}{1-P(x)} \tag{1.9}$$

它表示 x 的出现概率与不出现概率之比，显然随 $P(x)$的加大 $O(x)$也加大，而且

当 $P(x)=0$ 时，有 $O(x)=0$ （1.10）

当 $P(x)=1$ 时，有 $O(x)=\infty$ （1.11）

于是，取值于[0,1]的 $P(x)$被放大为取值于$[0,\infty]$的 $O(x)$。

（2）充分性度量：充分性度量定义为

$$\mathrm{LS}=\frac{P(E\mid H)}{P(E\mid \neg H)} \tag{1.12}$$

它表示 E 对 H 的支持程度，由专家给出。其中 E 代表证据，H 代表结论。

（3）必要性度量：必要性度量定义为

$$\mathrm{LN}=\frac{P(\neg E\mid H)}{P(\neg E\mid \neg H)}=\frac{1-P(E\mid H)}{1-P(E\mid \neg H)} \tag{1.13}$$

它表示 $\neg E$ 对 H 的支持程度，即 E 对 H 为真的必要性程度，也是由专家凭经验给出的。

2．证据的不确定性描述

在主观贝叶斯方法中，证据 E 的不确定性用证据的概率 $P(E)$表示，或者用证据 E 的几率 $O(E)$表示。$O(E)$与 $P(E)$的关系如下：$O(E)=\dfrac{P(E)}{1-P(E)}$。下面是几种典型情况下 $O(E)$与 $P(E)$的取值：

（1）当 E 为真时，$P(E)=1$，$O(E)=\infty$；

（2）当 E 为假时，$P(E)=0$，$O(E)=0$；

（3）当 E 不确定时，$P(E)$和 $O(E)$分别取 E 的先验概率和先验几率。

3．基于主观贝叶斯方法的不确定性推理

在主观贝叶斯方法中，知识是用产生式规则表示的，具体形式为：

IF E THEN　(LS,LN) H　($P(H)$)

LS，LN 是充分性度量和必要性度量，由领域专家给出。证据 E 的概率为 $P(E)$，结论 H 有一个先验概率 $P(H)$，表示在没有任何专门证据的情况下结论为真的概率，其值同样也由专家给出。主观贝叶斯方法的推理就是由 $P(E)$，利用规则的 LS 和 LN，把结论 H 的先验概率

$P(H)$更新为后验概率求出 $P(H|E)$或 $P(H\mid\neg E)$ 的过程。而一条规则的前件有可能肯定存在，也可能肯定不存在，或者不确定，而且在不同情况下求解后验概率的方法也不相同，以下分别予以讨论。

（1）证据 E 确定必出现时，即 $P(E)=1$，由贝叶斯公式：

$$P(H\mid E)=P(E\mid H)\times P(H)/P(E) \tag{1.14}$$

$$P(\neg H\mid E)=P(E\mid\neg H)\times P(\neg H)/P(E) \tag{1.15}$$

由以上两式可得：

$$\frac{P(H\mid E)}{P(\neg H\mid E)}=\frac{P(E\mid H)}{P(E\mid\neg H)}\times\frac{P(H)}{P(\neg H)} \tag{1.16}$$

即有：

$$O(H\mid E)=\mathrm{LS}\times O(H) \tag{1.17}$$

若需要以概率的形式表示，再由公式：

$$P(E)=\frac{O(E)}{1+O(E)} \tag{1.18}$$

计算出：

$$P(H\mid E)=\frac{\mathrm{LS}\times P(H)}{(\mathrm{LS}-1)\times P(H)+1} \tag{1.19}$$

这就是把先验概率 $P(H)$更新为后验概率 $P(H|E)$的计算公式。

（2）证据 E 确定必不出现时，即 $P(E)=0$，采用和上述类似的方法可得：

$$O(H\mid\neg E)=\mathrm{LN}\times O(H) \tag{1.20}$$

从而

$$P(H\mid\neg E)=\frac{\mathrm{LN}\times P(H)}{(\mathrm{LN}-1)\times P(H)+1} \tag{1.21}$$

这就是把先验概率 $P(H)$更新为后验概率 $P(H\mid\neg E)$ 的计算公式。

（3）当证据 E 不确定时，即在观察 S 下，证据 E 的概率 $P(E|S)$为：

$$0<P(E\mid S)<1 \tag{1.22}$$

所以就不能用上面的公式计算后验概率，可用 Duda 于 1976 年给出的公式：

$$P(H\mid S)=P(H\mid E)\times P(E\mid S)+P(H\mid\neg E)\times P(\neg E\mid S) \tag{1.23}$$

来计算出后验概率。可分为如下四种情况。

① 当 $P(E\mid S)=1$ 时，$P(\neg E\mid S)=0$，所以，

$$P(H\mid S)=P(H\mid E)=\frac{\mathrm{LS}\times P(H)}{(\mathrm{LS}-1)\times P(H)+1} \tag{1.24}$$

这就是证据肯定存在的情况。

② 当 $P(E\mid S)=0$ 时， $P(\neg E\mid S)=1$，所以，

$$P(H\mid S)=P(H\mid \neg E)=\frac{\mathrm{LN}\times P(H)}{(\mathrm{LN}-1)\times P(H)+1} \tag{1.25}$$

这就是证据肯定不存在的情况。

③ 当 $P(E\mid S)=P(E)$ 时，E 与 S 无关，利用全概率公式有：

$$P(H\mid S)=P(H\mid E)\times P(E)\times P(H\mid \neg E)\times P(\neg E)=P(H) \tag{1.26}$$

④ 当 $P(E\mid S)$ 为其他值时，通过分段线性插值的方法，就可以得到计算 $P(H\mid S)$ 的公式，即：

$$P(H\mid S)=\begin{cases}P(H\mid \neg E)+\dfrac{P(H)-P(H\mid \neg E)}{P(E)}\times P(E\mid S), & 若0\leqslant P(E\mid S)<P(E)\\ P(H)+\dfrac{P(H\mid E)-P(H)}{1-P(E)}\times[P(E\mid S)-P(E)], & 若0\leqslant P(E\mid S)<1\end{cases} \tag{1.27}$$

该公式称为 EH 公式。

对于初始证据，由于其不确定性是用可信度 $C(E|S)$给出的，并且为方便用户回答，采用 –5～5 这 11 个整数之一作为证据的可信度，用户可以根据实际情况从中选择。可信度 $C(E|S)$和概率 $P(E|S)$的对应关系如下：

$C(E|S)$=–5，表示在观察 S 下证据 E 肯定不存在，即 $P(E|S)$=0。

$C(E|S)$=0，表示 S 与 E 无关，即 $P(E|S)$= $P(E)$。

$C(E|S)$=5，表示在观察 S 下证据 E 肯定存在，即 $P(E|S)$=1。

$C(E|S)$为其他数时与 $P(E|S)$的对应关系，可通过对上述 3 点进行分段线性插值得到：

$$P(E\mid S)=\begin{cases}\dfrac{C(E\mid S)+P(E)[5-C(E\mid S)]}{5} & 0\leqslant C(E\mid S)\leqslant 5\\ \dfrac{P(E)[5+C(E\mid S)]}{5} & -5\leqslant C(E\mid S)<0\end{cases} \tag{1.28}$$

这样，用户只要对初始证据给出相应的可信度 $C(E|S)$，把 $P(E|S)$与 $C(E|S)$的对应关系转换公式代入 EH 公式，就可以得到用可信度 $C(E|S)$计算 $P(H|S)$的公式：

$$P(H\mid S)=\begin{cases}P(H\mid \neg E)+\dfrac{P(H)-P(H\mid \neg E)}{P(E)}\times[C(E\mid S)/5+1], & 若C(E\mid S)\leqslant 0\\ P(H)+[P(H\mid E)-P(H)]\times C(E\mid S)/5, & 若C(E\mid S)>0\end{cases} \tag{1.29}$$

该公式称为 CP 公式。

这样，当用初始证据进行推理时，根据用户告知的 $C(E|S)$，通过运用 CP 公式就可以求出 $P(H|S)$；当用推理过程中得到的中间结论作为证据进行推理时，通过运用 EH 公式就可求出

$P(H|S)$。

4．证据为若干证据的组合

若有 n 个证据 $E_i(i=1,2,\cdots,n)$ 对假设 H 都有某种程度的影响（即存在规则 $E_1 \to H$，$E_2 \to H,\cdots,E_n \to H$，$E_i$ 之间相互独立且对每个 E_i 都有相应的观察 S_i 与之对应），只要先对每条规则分别求出 $O(H|S_i)$，则这些独立证据的组合所得到的 H 的后验几率 $O(H \mid S_1 \& S_2 \& \cdots \& S_n)$ 为：

$$O(H \mid S_1 \& S_2 \& \cdots \& S_n) = \frac{O(H \mid S_1)}{O(H)} \times \frac{O(H \mid S_2)}{O(H)} \times \cdots \times \frac{O(H \mid S_n)}{O(H)} \times O(H) \qquad (1.30)$$

这只是证据组合的其中一种，另外还有证据的合取、证据的析取等。

主观贝叶斯方法是在概率论的基础上发展起来的，具有较完善的理论基础，且知识的输入转化为对 LS 和 LN 的赋值，这就避免了大量的数据统计工作，是一种比较实用且较灵活的不确定性推理方法。但是，它在要求专家给出 LS 和 LN 的同时，还要求给出先验概率 $P(H)$，而且要求事件间相互独立，这仍然比较困难，从而也就限制了它的应用。

1.3.2 模糊逻辑推理[8]

模糊逻辑推理与主观贝叶斯推理有着实质性的区别。主观贝叶斯推理的理论基础是概率论，它所研究的事件本身有明确的含义，只是由于发生的条件不充分，使得在条件与事件之间不能出现确定的因果关系，从而在事件的出现与否上表现出不确定性。那些推理模型是对这种不确定性，即随机性的表示与处理。模糊推理的理论基础是模糊集理论，以及在此基础上发展起来的模糊逻辑。它所处理的事物自身是模糊的，概念本身没有明确的外延，一个对象是否符合这个概念难以明确地判定。模糊推理是对这种不确定性，即模糊性的表示与处理。

模糊逻辑推理是基于模糊性知识(模糊规则)的一种近似推理，一般采用 Zadeh 提出的语言变量、语言值、模糊集和模糊关系合成的方法进行推理。

（1）语言变量：语言变量一般用来描述那些不精确的事件或现象，就是我们通常所说的属性名。例如，“年龄”就是一个语言变量，其取值可为“老”、“中”、“青”等。这些值可看成是论域 $U=[0,150]$ 上模糊子集的标名，而数字变量 $u \in [0,150]$ 称为基变量。

（2）证据模糊性及模糊规则的表示：命题的模糊性可用模糊子集来描述。例如，设有命题“张三比较小”，则可以表示为：

$$\text{Zhangsan} \quad \text{is} \quad \tilde{A}$$

其中，$\tilde{A}=$“比较小”$=1/1+1/2+0.5/3+0.2/4+0.1/5+0/6=(1,1,0.5,0.2,0.1,0)$ 是一个模糊子集，代表“比较小”这个模糊概念。

一条模糊规则实际上是刻画了其前件中的模糊集与结论中的模糊集之间的一种对应关

系。Zadeh 认为，这种对应关系是两个集合间的一种模糊关系，因而它也可以表示为模糊集合。特别地，对于有限集，这个模糊集合就可以表示为一个模糊矩阵。例如，有规则：

$$R:\text{IF}\quad \text{Zhangsan}\quad \text{is}\ \tilde{A}\quad \text{THEN Lisi}\quad \text{is}\ \tilde{B}$$

其中，$\tilde{A}$ 和 $\tilde{B}$ 都是模糊子集，表示模糊概念。这个规则就表示了 $\tilde{A}$ 和 $\tilde{B}$ 之间的一种模糊关系，$\tilde{R}$ 表示这个模糊关系，则 $\tilde{R}$ 也可以表示为一个模糊子集。于是：

$$\begin{aligned}\tilde{R} &= \mu_{\tilde{R}}(u_1,v_1)/(u_1,v_1)+\mu_{\tilde{R}}(u_1,v_2)/(u_1,v_2)+\\ &\quad \cdots+\mu_{\tilde{R}}(u_i,v_j)/(u_i,v_j)+\cdots\\ &= \int_{U\times V}\mu_{\tilde{R}}(u,v)/(u,v)\end{aligned} \tag{1.31}$$

其中，U、V 分别为模糊集合 $\tilde{A}$，$\tilde{B}$ 所属的论域，$\mu_{\tilde{R}}(u_i,v_j)(i,j=1,2,\cdots)$ 是元素 $\mu_{\tilde{R}}(u_i,v_j)$ 对于 $\tilde{R}$ 的隶属度。

为求得隶属度 $\mu_{\tilde{R}}(u_i,v_j)$，Zadeh 给出了一种方法：

$$\mu_{\tilde{R}}(u_i,v_j)=(\mu_{\tilde{A}}(u_i)\wedge\mu_{\tilde{B}}(v_j))\vee(1-\mu_{\tilde{A}}(u_i))(i,j=1,2,\cdots) \tag{1.32}$$

其中，$\wedge$、$\vee$ 分别代表取最小值和取最大值，即 min、max。如果 $\tilde{A}$，$\tilde{B}$ 都是有限集，则 $\tilde{R}$ 就是一个矩阵。

这样，一条模糊规则 R 就可以用隶属度 $\mu_{\tilde{R}}(u_i,v_j)$ 刻画的模糊集合来描述。

（3）模糊推理：模糊推理有很多种，在这里我们仅介绍一种简单而常用的方法。模糊推理可以通过模糊关系的合成来进行。假设有规则：

$$R:\text{IF}\quad x\ \text{is}\ \tilde{A}\quad \text{THEN}\quad y\quad \text{is}\ \tilde{B}$$

其推理模式为：

$$\tilde{\boldsymbol{B}}=\tilde{\boldsymbol{A}}\circ\tilde{\boldsymbol{R}}=\begin{pmatrix}a_{11} & a_{12} & \cdots & a_{1k}\\ a_{21} & a_{22} & \cdots & a_{2k}\\ \cdots & \cdots & \cdots & \cdots\\ a_{n1} & a_{n2} & \cdots & a_{nk}\end{pmatrix}\circ\begin{pmatrix}r_{11} & r_{12} & \cdots & r_{1m}\\ r_{21} & r_{22} & \cdots & r_{2m}\\ \cdots & \cdots & \cdots & \cdots\\ r_{k1} & r_{k2} & \cdots & r_{km}\end{pmatrix}=(b_{ij})_{n\times m} \tag{1.33}$$

其中，

$$b_{ij}=\bigvee_{i=1}^{k}a_{il}\wedge r_{lj}(i=1,2,\cdots,n;\ j=1,2,\cdots,m) \tag{1.34}$$

一般情况下，n=1。

这样，$\tilde{R}$ 就是规则 R 按上述方法导出的模糊集合，而 $\tilde{B}$ 就是所推的结论。当然，它仍是一个模糊集合。如果需要，可再将它翻译为自然语言的形式。

1.3.3 证据理论[8]

Dempster 和 Shafer 提出的证据理论，可用来处理由不知道所引起的不确定性。采用信任函数而不是概率作为不确定性度量，通过对一些事件的概率加以约束来建立信任函数而不必说明精确的难于获得的概率，当这种约束限制为严格的概率时，证据理论就退化为概率论了。

1．证据理论的原理

若用 U 表示所有可能的假设集合，而 U 的元素间是互斥的，对任一 A 属于 U 的子集，命题 A 表示了某些假设的集合（这样的命题间不再有互斥性）。例如，针对医疗诊断问题，U 就是所有可能疾病（假设）的集合，诊断结果必是 U 中确定的元素构成的。A 表示某一种（单元素）或某些种疾病。医生为了进行诊断所进行的各种检查就称做证据，有的证据所支持的常不只是一种疾病而是多种疾病，即 U 的一子集 A，子集构成求解问题的各种解答，证据理论就是通过定义在这些子集上的几种信任函数，来计算子集为真的可信度的。例如，医疗诊断中的证据“流鼻涕”，有可能是“感冒”，也有可能是“过敏性鼻炎”引起的，则有 A={“感冒”，“过敏性鼻炎”}。证据理论就是求 A 作为所有疾病集合子集的可信度。

1）基本概率分配函数

首先在 U 的幂集 2^U 上定义一个基本概率分配函数（Function of Basic Probability Assignment）：

$$m: 2^U \to [0,1] \tag{1.35}$$

满足 $m(\phi)=0$，$\sum_{A\subseteq U} m(A)=1$。

基本概率分配函数值一般由主观给出，一般是某种可信度，所以概率分配函数也被称为可信度分配函数。

2）信任函数（Function of Belief）

$$\mathrm{Bel}: 2^U \to [0,1] \text{ 且 } \mathrm{Bel}(A)=\sum_{B\subseteq A} m(B) \text{,其中 } A\in 2^U \tag{1.36}$$

子集 A 的信任函数的值是 A 的所有子集的基本概率分配函数值的和，用来表示对 A 的总信任。信任函数表示对 A 为真的信任程度，又称下限函数。信任函数具有如下性质：

- $\mathrm{Bel}(\phi)=0$，$\mathrm{Bel}(U)=1$，且对于 2^U 中的任意元素 A，有 0≤Bel(A) ≤1。
- 单元素集上 m 与 Bel 是相等的，即若 A 是单元素集，则 $m(A)$=Bel(A)。
- 信任函数为递增函数，即若 $A_1 \subseteq A_2 \subseteq U$，则 Bel($A_1$)≤Bel($A_2$)。

3）似然函数(Plausible function)

$$\mathrm{Pl}(A)=1-\mathrm{Bel}(A') \tag{1.37}$$

其中，A' 为 A 的补集。表示对 A 非假的信任程度，也就是所有与 A 相交的子集的基本概率分配函数的和。似然函数又称为上限函数。似然函数有下列性质：

- $\mathrm{Pl}(A)=\sum_{A\cap B\neq\phi} m(B)$ （1.38）
- $0\leqslant \mathrm{Bel}(A)\leqslant \mathrm{Pl}(A)\leqslant 1$ （1.39）
- $\mathrm{Pl}(A)+\mathrm{Pl}(A')\geqslant 1$ （1.40）
- $\mathrm{Pl}(A)-\mathrm{Bel}(A)$表示了既不信任 A 也不信任 $\neg A$ 的一种度量，可表示对不知道的度量。

一般用信任区间 $[\mathrm{Bel}(A),\mathrm{Pl}(A)]$ 来描述 A 的不确定性。$\mathrm{Bel}(A)$表示度量的下限，$\mathrm{Pl}(A)$表示度量的上限。实际上 m、Bel、Pl 只要知其一，必可求得另两个，但三个函数有不同的含义。

4）Dempster 组合规则

（1）基本的组合规则：设 $m_1(A)$和 $m_2(A)\,(A\in 2^U)$ 是 U 基于不同证据的两个基本概率分配函数。则将二者可按下面的 Dempster 组合规则合并：

$$m(A)=\sum_{B\cap C=A} m_1(B)m_2(C) \tag{1.41}$$

该表达式一般称为 m_1 与 m_2 的正交和，并记为 $m=m_1\oplus m_2$。

组合后的 $m(A)$满足：$\sum_{A\subseteq U} m(A)=1$。

（2）含冲突修正的组合规则：在上面的基本组合规则中，若 B 和 C 的交集为空集，这时将 Dempster 组合规则进行如下修正。

$$m(A)=\begin{cases}0, & 若A=\phi\\ K\sum_{B\cap C=A} m_1(B)m_2(C) & 若A\neq\phi\end{cases} \tag{1.42}$$

其中，K 为规范数，并且

$$K=\left(1-\sum_{B\cap C=\phi} m_1(B)m_2(C)\right)^{-1} \tag{1.43}$$

规范数 K 的引入，实际上是把空集所丢弃的正交和按比例地补到非空集上，使所有的 $m(A)$仍然满足：$\sum_{A\subseteq U} m(A)=1$。

2．证据推理模式

基于证据理论的不确定性推理，大体可分为以下步骤：

（1）建立问题的识别集合 U；

（2）给幂集 2^U 定义基本概率分配函数；

（3）计算所关心的子集 $A \in 2^U$（即 U 的子集）的信任函数值 Bel(A)、似然函数值 Pl(A)；

（4）由 Bel(A)和 Pl(A)得出结论。

1.4 挖掘不确定知识的方法

普遍认为，所谓数据挖掘，就是从大量的、不完全的、有噪声的、模糊的、随机的数据中，提取隐含在其中的、人们事先不知道的，但又是潜在有用的信息和知识的过程。人们把原始数据看做是形成知识的源泉，就像从矿石中采矿一样。原始数据可以是结构化的，也可以是半结构化的；发现知识的方法可以是数学的，也可以是非数学的，可以是演绎的，也可以是归纳的；发现的知识可以被用于信息管理、查询优化、决策支持、过程控制，还可以用于数据自身的维护。

通过 10 多年的研究，人们已经提出了很多有效的数据挖掘方法和工具，但与人们对数据挖掘的普遍期望相比，即希望挖掘过程自动化、智能化，希望所发现的知识是客观的、精确的且恒定的，数据挖掘的研究现状还有很大差距。其中的原因当然很多，但一个重要的原因是，人们忽视了数据挖掘过程中的不确定性和发现知识的不确定性。

数据挖掘中，大多数的挖掘任务都是面向特定的应用领域的。描述和确定挖掘任务时，往往要求用户具备详尽的领域知识和背景知识。由于用户的常识和背景知识本身具有不确定性，因此，在最初的任务描述中就已经存在不确定性了。

在数据收集阶段，不同的用户可能会对不同层次、不同类型的知识感兴趣，收集哪些原始数据用于数据挖掘本身就很难确定。即使对同一个用户而言，由于无法预知待发现知识的类型和性质，选择数据时也会具有很大的随机性或试探性。

数据预处理时，对空缺值、测量误差、噪声数据等的处理也可能影响最终的挖掘结果。后续的数据挖掘过程，本质上是一个实验性的数据分析过程，即假设数据已经被收集好，关注的只是如何发现其中的信息和知识。但如果预处理没能给出高质量的数据集，其最终的结果只能是“垃圾进，垃圾出”。其次，大规模实际数据集中，除了噪声、测量误差、丢失值以外，还存在许多不重要的或冗余的特征，这些不重要的或冗余的特征不仅不能提高挖掘结果的有效性和正确性，反而会混淆数据分布，降低数据挖掘的效率和挖掘结果的可理解性。然

而，如何根据挖掘任务填补丢失值，修正误差，剔除噪声数据，以及选择有助于呈现数据分布的重要特征子集等，本身就有不确定性，尤其当用户不清楚要发现的知识性质时，更是如此。

根据挖掘任务，设计、选择并实现有效的数据挖掘算法是数据挖掘过程中的一个关键步骤。一般来说，大多数的数据挖掘算法都是基于机器学习、模式识别、统计分析等方法，分别从不同角度进行知识或模式的抽取，当用户不清楚感兴趣的知识性质时，选择哪种挖掘算法具有不确定性。另外，大多数挖掘算法要求用户预先设定算法参数，且数据挖掘结果的有效性依赖参数的合理设置。然而实际应用中，待挖掘的数据集通常很庞大，数据分布特性又是未知的。在这种情况下，让用户预先设置算法参数是非常困难的，用户只能根据自己对挖掘任务的理解或有限的背景知识随机选取一些参数，由此导致挖掘结果的不确定性。

数据挖掘的最终目的是向用户提供新颖的、潜在有用的知识和模式，如何让用户快速、准确地理解和评估所获得的知识显然是非常重要的。要求用户能合理地归纳、简化所得的知识模式，并以人们易于理解的形式加以描述，如可视化方法和自然语言表示方法。可视化方法可以形象直观地表示数据间的内在关联，但通常不适用于高维知识表示；自然语言方法符合人们的思维习惯，其最小单位是语言值，它对应的定性概念是人类思维的基本单元。由于构成知识的定性概念具有内在的不确定性，采用自然语言解释所发现的知识面临的最主要的问题是，如何描述定性概念的不确定性及如何实现从数据到定性概念的不确定性转换。此外，挖掘结果的简约性与挖掘结果的准确性这两者之间也需要折中。对于所发现知识的评价来说，虽然人们已经提出许多客观的评价度量，如评价聚类知识的紧凑性和可分性度量、关联知识的支持度和置信度等，但知识的可用性或新颖性等评价准则明显取决于用户感兴趣的程度或用户的背景知识，具有主观性。因此，知识的解释与评价步骤也存在不确定性。所以说，数据挖掘的过程是一个不确定的过程。

事实上，不仅数据挖掘过程中有很多不确定性，发现的知识本身也有不确定性。数据挖掘主要是以隐含在大量数据中的共同性知识和差异性知识作为研究对象的。主要包括广义知识、分类和聚类知识、关联知识、预测知识、离群知识。不同类型的知识虽然各有特点，但也有内在的关联性。分类和聚类知识不仅是一种重要的知识类型，也是数据挖掘系统中发现广义知识、关联知识等共同性知识和离群知识等差异性知识的先决条件，其重要性体现在：关联知识是对数据的概括和抽象；离群知识是对差异和极端特性的描述；而分类和聚类知识不仅可以实现数据的有用概括和描述，而且在把整个数据集划分成相似的子集之后，采用面向属性的归纳等其他数据挖掘工具更容易在分类和聚类知识的基础上发现重要的规则和模式。此外，分类和聚类知识发现系统利用分类和聚类知识实现数值型属性的离散化，概念层次的自动生成等基本任务。因此，数据挖掘本质上是一个从相同数据源中抽取共同性知识和差异性知识的认知过程。共同性知识和差异性知识往往是针对信息粒度或抽象程度而言的，

某一粒度的共同性知识很可能是另一更高粒度上的差异性知识，反之亦然。因此，所发现的知识具有相对性。

1．不确定条件下的自适应知识学习算法

不确定性条件下的数据自适应知识学习方法，或者称为主动式学习方法，是人工智能知识获取研究中的一个难题。在学习过程中，如果能够摆脱对先验知识的依赖，实现自适应知识获取过程，无疑将对知识学习理论的发展和应用起到重要的推动作用。

参考文献[9]通过构造一种度量决策表和决策规则不确定性的方法，对二者不确定性度量的关系进行研究，将决策表的局部最小确定性作为控制规则生成过程中的阈值来控制规则生成。这样就得到了一种在不确定性条件下，完全由数据自主控制规则生成的知识学习方法，提出了一种不确定性条件下的自适应知识学习方法。该方法能够在不确定性条件下获取规则，从某种程度上摆脱了知识获取过程中对领域先验知识的依赖。

算法：自适应知识获取算法

输入：决策表 $S=<U,A,V,f>$，其中 U 是论域，$A=C\cup D$ 是属性集合，子集 C 和 D 分别为条件属性集和决策属性集。

输出：默认规则集。

Step1：根据条件属性计算决策表 S 的不可区分关系，即条件属性对决策表 S 的划分。

$E_{(k,c)}=U/\mathrm{IND}(C)$，$k=1,\cdots,U/\mathrm{IND}(C)$。根据定义计算出决策表 S 的局部最小确定性 α_c，并以 α_c 作为控制规则生成的阈值。

Step2：$|E_{(k,c)}\cap X_j|/|E_{(k,c)}|\geqslant\alpha_c$，则根据决策表 S 的可辨识矩阵产生相应的默认规则。

Rule：$\mathrm{Des}(E_{(k,c)},C)\rightarrow\mathrm{Des}(X_j,D)$ ｜ $|E_{(k,c)}\cap X_j|/|E_{(k,c)}|$

其中，$|E_{(k,c)}\cap X_j|/|E_{(k,c)}|$ 是规则 $\mathrm{Des}(E_{(k,c)},C)\rightarrow\mathrm{Des}(X_j,D)$ 的可信度因子。

Step3：将决策表 S 加入决策表集合 $\psi=\{S\}$。

Step4：如果 $\psi=\phi$，则结束；否则从 Ψ 中取出一个决策表 $S^*=<U,R^*,V^*,f^*>$，计算其属性核 $\mathrm{CORE}(C^*)$。通过删除某一核属性（如 C_{cut}），可以得到条件属性上的投影 $C_{\mathrm{Pr}}=C^*-C_{\mathrm{cut}}$，其中，$r=1,\cdots,|\mathrm{CORE}(C^*)|$，$C^*$ 为该决策表的条件属性集合，C_{cut} 是被删除的核属性。对每个投影 C_{Pr} 做如下处理。

① 如果 $C_{\mathrm{Pr}}\neq\phi$，则对该投影不做任何操作；否则，做下面的 4 步操作。

② 将投影得到的新决策表 $S'=(U,R',V',f')$ 加入 Ψ，$\psi=\psi\cup\{S'\}$，其中 $A'=C_{\mathrm{Pr}}\cup D$。

③ 根据条件属性计算投影 C_{Pr} 的不可区分关系，即条件属性对该投影决策表 S' 的划分：

$$E_{(k,C_{\mathrm{Pr}})}(E_{(k,C_{\mathrm{Pr}})}\in U|\mathrm{IND}(C_{\mathrm{Pr}}),k=1,\cdots,|U/\mathrm{IND}(C_{\mathrm{Pr}})|)$$

④ 如果$|E_{(k,C_{\Pr})} \cap X_j| / |E_{(k,C_{\Pr})}| \geqslant \alpha_c$，则得到相应的默认规则：

$$\text{Rule}': \text{Des}(E_{(k,C_{\Pr})}, C_{\Pr}) \rightarrow \text{Des}(X_j, D) \quad | \quad |E_{(k,C_{\Pr})} \cap X_j| / |E_{(k,C_{\Pr})}|$$

⑤ 为每条默认规则 Rule′ 构造封锁该规则的事实。如果存在 E_i，$E_i \in U/\text{IND}(C)$，并且 E_i 是 $E_{(k,C_{\Pr})}$ 的子集，$E_i \cap X_j = \phi$。则形成事实：

$$F': \text{Des}(E_i, C_{\text{cut}}) \rightarrow \text{NOT}(\text{Rule}')$$

Step5：转 Step 4。

2．不确定性文本聚类方法

目前典型的聚类算法均需不同程度地选择阈值，阈值的选择将直接影响聚类的质量，而对于文本这种特殊的对象，其维度高，且具有稀疏性，不同的簇之间相似度的差异比较大，如果采用固定的阈值来控制文本聚类过程，会导致较差的聚类结果。有研究者提出了一种自动调节阈值的方法，但是该方法主要是在聚类的不同层次设定不同的阈值，而阈值的设定本身仍需要用户指定。

目前，诸多的聚类算法中都需要用户指定相关的阈值，最典型的是 DBSCAN 算法中需要用户指定两个参数作为测试区域的半径和成为高密度区域的条件（指定半径区域内的对象数目）。由用户指定参数有其不足之处：需要用户对整个对象的分布情况有深入的了解，但对于文本这种高维度的对象来说，这是不太可能的；另外用一个固定的参数来施加到整个集合上显然是不合理的，因为文本集合中隐含的簇模式很可能具有不同密度。

参考文献[10]是通过应用多项式拟合曲线技术，寻找曲线拐点来发现阈值的方法，从而代替了用户指定阈值的方法。这样，针对一个对象与其他对象的相似度，可以自动地选定阈值，以适应不同的密度情况，求得更好的聚类结果。

因此，根据曲线的多项式拟合技术提出的自动发现阈值的方法，不仅替代了用户指定参数的过程，而且自动获得了随数据分布动态变化的阈值，使聚类过程更加自动化和智能化。自动发现阈值的基本思想是：对于一个文本，如果将它与其他文本的相似度递减排序，与其相似的文本（即与该文本在一个隐含的簇里的文本）之间的相似度较之与其不相似文本（与该文本不在一个隐含的簇里的文本）之间的相似度在总体上一定有一个比较大的区别。采用三次多项式方程来拟合这些以相似度为坐标的点，通过求得拟合曲线的拐点确定相应的阈值。

3．不确定性关联知识的发现

关联知识是数据挖掘中一个重要的知识类型，最早由 R.Agrawal 等人在研究超市交易数据库时提出，用来描述属性之间的依赖关系。

在关联规则挖掘方法中，通常有两个阈值需要设置，一个是最小支持度，一个是最小可信度。但是，对于一个面向领域的问题来说，往往很难设置合适的阈值。为了避免生成不需要的规则，人们引入了各种新的阈值以加强对关联规则的评判。在这当中，兴趣度的提出是一个比较瞩目的观点。基于兴趣度的关联规则发现算法也相继提出。下面的算法就是一个基于兴趣度的关联规则发现算法[11]。

Step 1：包含正项的频繁项集生成阶段。利用已有的计算频繁项集的方法，计算出正项的频繁项集及相应的支持度。

Step 2：对 Step 1 产生的所有频繁项集，使用可信度和兴趣度作为阈值对频繁项集进行过滤，产生通常意义上的关联规则。

Step 3：对 Step 2 中由于兴趣度小于 1 而被淘汰下来的频繁项集，考虑其带负项的关联规则构成的可能性；若其构成的带负项的关联规则满足可信度和兴趣度阈值，则生成该关联规则。相对于其他的关联规则发现算法，这个算法的特色在于当所发现出来的规则并不令人感兴趣时，它能够自动考虑引入反向项集来产生或许更令人感兴趣的关联规则。

1.5 小结

不确定性是客观世界固有的属性，通常表现为随机性、模糊性。为了能够准确地度量这些不确定性，根据其特性，一般采用概率论、模糊理论和粗糙集理论等数学方法。在对不确定性度量的基础上，要使不确定性能够传播和更新，就需要对不确定性进行一定程度的推理，即新的不确定性知识的获取过程。它是建立在不确定性知识和证据基础上的推理。例如，不完备、不精确知识的推理，模糊知识的推理等。实际上，它是一种从不确定的初始证据出发，通过运用不确定性知识，最终推出具有一定程度的不确定性但却又是合理或基本合理的结论的思维过程。不确定性推理的方法主要包括主观贝叶斯推理、模糊逻辑推理和证据理论。对于不确定知识的发现，研究者们提出了许多方法。例如，不确定条件下的自适应知识获取、不确定性聚类方法和不确定性关联知识的发现等。

参 考 文 献

[1] 李德毅，杜鹢．不确定性人工智能．北京：国防工业出版社，2005．

[2] 王士同等．人工智能教程．北京：电子工业出版社，2001．

[3] Zadeh L A．Fuzzy Sets．Information and Control，1965(8):338-353．

[4] Pawlak Z. Rough Sets. International Journal of Computer and Information Science，1982(11):341-356.
[5] 史忠植．知识发现．北京：清华大学出版社，2002.
[6] 张仰森．人工智能原理与应用．北京：高等教育出版社，2004.
[7] 劭军力，张景，魏长华．人工智能基础．北京：电子工业出版社，2000.
[8] 蔡自兴．人工智能及其应用．北京：清华大学出版社，2000.
[9] 王国胤，何晓．一种不确定性条件下的自主式知识学习模型．软件学报，2003：1096-1102.
[10] 张猛，王大玲，于戈．一种基于自动阈值发现的文本聚类方法．计算机研究与发展，2004：1749-1753.
[11] 周皓峰，朱扬勇，施伯乐．一个基于兴趣度的关联规则采掘算法．计算机研究与发展，2002：450-457.

Chapter 2

第2章 模糊集与粗糙集理论

2.1 模糊集合及其运算[1~3]

在经典集合论中，任何一个元素与任何一个集合之间的关系，只有“属于”或“不属于”两种，两者必居其一，而且只居其一，绝对不允许模棱两可。用特征函数描述经典集合，充分显示出它的“非此即彼”的特征。以经典集合论为理论基础的经典数学，在处理清晰的、确定性的问题时，达到了高度的严密性和精确性。但是用它处理具有模糊性的问题时，就显得无能为力，甚至出现自相矛盾的局面。以至不少科学领域成为经典数学的禁区。

我们知道，在思维中每一个概念都有一定的内涵和外延，它们是刻画概念的两个方面，概念的形成总是要以集合论为依托的。内涵就是集合的定义，外延就是组成集合的所有元素。经典集合的内涵和外延是明确的，具有明确的内涵和外延的概念都可以用经典集合去表示。例如，“不大于 10 的自然数”是一个清晰的概念，它可以用经典集合表示为：

$$A=\{x,x\in N,x\leqslant 10\} \tag{2.1}$$

又如“男子”、“女子”也都是清晰概念，我们可以在人群中很容易地进行区分。但是，日常生活中也存在着大量的模糊概念，它们没有明确的外延。例如，“比 5 大得多的整数”就是一个模糊概念，因为它没有明确的外延，即我们无法划定一个明朗的界限，使得在这个界限内的所有整数，都是比 5 大得多的，而在界限外的所有整数，都不是比 5 大得多的整数。

我们只能说某数（如 100）属于“比 5 大得多”的程度要比某数（如 50）属于“比 5 大得多”的程度高。又如“青年人”、“老年人”、“高个子”、“大胖子”等都是一些模糊概念，都没有明确的外延。模糊概念是不能用经典集合来描述的，这是因为不能绝对地划分“属于”、“不属于”，只能说属于的程度是多少。

那么，怎样描述一个模糊概念呢？Zadeh（扎德）仿照用特征函数表示经典集合的方法，用隶属函数表示模糊集合，就是把特征函数的取值范围，从{0，1}的两个位扩大到[0，1]闭区间内连续取值，即：

$$\Psi_A : U \to [0,1] \tag{2.2}$$

扎德就是从这一点取得突破，利用经典集合这一工具，实现定量地描述模糊集合。为了有所区别，我们特意将模糊集合的特征函数改称做隶属函数，将 Ψ_A 改写为 μ_A，于是引出如下定义。

定义 2.1　论域 U 中的模糊集合 A，是以隶属函数 μ_A 为表征的集合，即：

$$\mu_A : U \to [0,1] \tag{2.3}$$

对任意 $u \in U$，有 $u \to \mu_A(u)$，$\mu_A(u) \in [0,1]$，称 $\mu_A(u)$ 为元素 u 对于 A 的隶属度。表示 u 属于 A 的程度。

2.1.1　模糊集合的概念[4]

定义 2.2　设 U 为论域。则一个定义在 U 上的模糊集合 F 可由隶属函数 $\mu_F : U \to [0,1]$ 来表征，这里 $\mu_F(u)$ 表示 $u \in U$ 在 F 上的隶属程度。

因为经典集合或普通集合的隶属函数只有两个取值{0,1}，故模糊集合可以看成是经典集合的推广。例如，下式给出了一个模糊集合 F，它表示远大于零的实数，即 $F = \{x \mid x \gg 0, x \in U\}$，其隶属函数为：

$$\mu_F(u) = \begin{cases} 0, & x \leqslant 0 \\ \dfrac{1}{1 + \dfrac{100}{x^2}}, & x > 0 \end{cases} \tag{2.4}$$

定义 2.3　支撑集（或简称支集），核和模糊单值的定义是：模糊集合 F 的支撑集是所有的 $u \in U$ 中，满足 $\mu_F(u) > 0$ 的那些点组成的明晰集合。模糊集合 F 的核是 $u \in U$ 中使得 $\mu_F(u)$ 取最大值的点。如果模糊集合 F 的支撑集在 U 上只含一个点，且有 $\mu_F = 1$，则 F 就称为模糊单值。

定义 2.4　设 A 和 B 是 U 上的两个模糊集合，则对所有的 $u \in U$，A 和 B 的交集是定义在 U 上的一个模糊集合，其隶属函数定义如下：

$$\mu_{A\cap B}(u)=\min\{\mu_A(u),\mu_B(u)\} \tag{2.5}$$

A 和 B 的并集是定义在 U 上的一个模糊集合，其隶属函数定义如下:

$$\mu_{A\cup B}(u)=\max\{\mu_A(u),\mu_B(u)\} \tag{2.6}$$

对所有的 $u\in U$， A 的补集 $\bar{A}$ 是定义在 U 上的一个模糊集合，其隶属函数定义如下：

$$\mu_{\bar{A}}(u)=1-\mu_A(u) \tag{2.7}$$

上述定义的模糊集合的并、交运算分别记为 $\cup$，$\cap$。

应该指出，在模糊集合理论中，上述的 max、min 常因实际的需要，而用三角模 S 和三角模 T 分别代替之。

常见的三角模 S 有：

$$S(a,b)=\begin{cases}\max\{a,b\}, & \text{模糊并}\\ a+b-a\bullet b, & \text{代数和}\\ \min\{1,a+b\}, & \text{有界和}\\ \left\{\begin{matrix}a,b=0\\ b,a=0\\ 0,a,b>0\end{matrix}\right\}, & \text{直和}\end{cases} \tag{2.8}$$

常见的三角模 T 有：

$$T(a,b)=\begin{cases}\min\{a,b\}, & \text{模糊交}\\ a\bullet b, & \text{代数乘}\\ \max\{0,a+b-1\}, & \text{有界乘}\\ \left\{\begin{matrix}a,b=1\\ b,a=1\\ 0,a,b<1\end{matrix}\right\}, & \text{直积}\end{cases} \tag{2.9}$$

定义 2.5 模糊数：设 A 为实数域 U 上的模糊子集，$\mu_A(x)$ 为其隶属函数，设 $\beta=\sup\mu_A(x)$（$\sup A$ 的上模，即 $\mu_A(x)$ 的极大值），若对任意 $\lambda\in(0,\beta)$，$A_\lambda=\{x\mid\mu_A(x)\geqslant\lambda\}$ 都是一个闭区间，则称 A 是一个模糊数。

由此有结论：

（1）具有连续隶属函数 $\mu_A(x)$ 的凸模糊集是模糊数；

（2）实数集 U 中的任意闭区间 $[a,b]$ 都是一个模糊数。可见，模糊数是区间数的推广，而区间数则是模糊数的特例。

2.1.2　模糊集合的运算[5]

定义 2.6　设U和V为两个论域，模糊关系R是积空间$U\times V$上的模糊集合，即当$u\in U$，$v\in V$时，R的隶属函数为$\mu_R(u,v)$。

定义 2.7　设R和S分别是$U\times V$和$U\times W$上的模糊关系，则R和S的合成$R\circ S$定义为$U\times W$上的一个模糊关系，其定义如下：

$$\mu_{R\circ S}(u,w)=\bigvee_{v\in V}(\mu_R(u,v)\wedge\mu_R(v,w)) \tag{2.10}$$

定义 2.8　语言变量：可用一个五元组$(x,T(x),U,G,M)$来表征，其中，x为变量名称；$T(x)$为x的术语集合，即x语言取值的集合。其中，x的每一个语言取值对应于一个在U上的模糊集合；U是论域；G为x语言取值的语法规则；M为解释x每个语言取值的语义规则。

上述定义可能会让人觉得语言变量是一个很复杂的概念，但事实并非如此。引入语言变量这个概念的目的只是要正式表明，一个变量是能够用普通语言中的词汇来作为它的取值的。例如，我们说“速度快”，则这里的变量“速度”就可以理解为一个语言变量，而“快”则是它在对于速度的论域中所取的一个模糊值。

定义 2.9　若一个变量能够用普通语言中的词（如小、大，快、慢等）来取值，则该变量就定义为语言变量。所用的词常是模糊集合的标识词。一个语言变量的取值既可为词也可为数据。

例如，语言变量“年龄”可用“年轻”、“中年”、“老年”来取值，也可用[0,120]上的任意值来取值。由此可见，语言变量是一个很重要的概念，它提供了量化语言描述的正规途径。

由于在语言描述中，我们常常用一些如“非常”、“或多或少”这一类的修饰词对主体词汇如“小”、“快”等进行修饰，因此，有必要对这类修饰词做一个正式的定义。

定义 2.10　设F是定义在U上的一个模糊集合（如$F=\text{small}$），则“非常F”也是定义在U上的一个模糊集合，其隶属函数为：

$$\mu_{\text{非常}F}(u)=(\mu_F(u))^2 \tag{2.11}$$

而“或多或少F”同样也是定义在U上的一个模糊集合，其隶属函数为：

$$\mu_{\text{或多或少}F}(u)=(\mu_F(u))^{1/2} \tag{2.12}$$

式中，$u\in U$。

在模糊逻辑和近似推理中有两种重要的推理方法，即所谓的广义取式（肯定前提）推理和广义拒式（肯定结论）推理。

定义 2.11　广义取式推理具有如下的推理过程。

前提 1：IF x is A,THEN y is B

前提 2：x is A'

结论：y is B'

定义 2.12 广义拒式推理具有如下的推理过程。

前提 1：IF x is A ，THEN y is B

前提 2：y is B'

结论：x is A'

其中，A' 、A 、B' 和 B 均为模糊集合，x 和 y 为语言变量。

定义 2.13 设 A 和 B 分别为定义在 U 和 V 上的模糊集合，则由 $A\rightarrow B$ 所表示的模糊蕴涵是定义在 $U\times V$ 上的一个特殊的模糊关系，其隶属函数定义如下。

$$\text{模糊与：}\ \mu_{A\rightarrow B}(u,v)=T(\mu_A(u),\mu_B(v)) \tag{2.13}$$

$$\text{模糊或：}\ \mu_{A\rightarrow B}(u,v)=S(\mu_A(u),\mu_B(v)) \tag{2.14}$$

$$\text{实质蕴涵：}\ \mu_{A\rightarrow B}(u,v)=S(\mu_{\bar{A}}(u),\mu_B(v)) \tag{2.15}$$

$$\text{命题演算：}\ \mu_{A\rightarrow B}(u,v)=S(\mu_{\bar{A}}(u),\mu_{A\wedge B}(v)) \tag{2.16}$$

$$\text{广义取式推理：}\ \mu_{A\rightarrow B}(u,v)=\vee\{c\in[0,1]\,|\,T(c,\mu_A(u))\leqslant\mu_B(v)\} \tag{2.17}$$

$$\text{广义拒式推理：}\ \mu_{A\rightarrow B}(u,v)=\wedge\{c\in[0,1]\,|\,S(c,\mu_B(v))\leqslant\mu_A(u)\} \tag{2.18}$$

一个模糊蕴涵 $A\rightarrow B$ 可以理解为这样一条“IF-THEN”：IF x is A，THEN y is B，其中 $x\in U$，$y\in V$，x 和 y 均为语言变量。式（2.13）～式（2.18）对应六种“IF-THEN”规则的表达式，而这些模糊规则是从直观推理准则和经典逻辑概念推广而来的。

2.1.3 模糊集合的扩张原理

扩张原理是将明晰集合的数学概念推广到模糊集合的重要手段，被广泛用于许多模糊实际应用之中。

定义 2.14 设 U 和 V 为两个论域，f 是从 U 到 V 的一个映射，对 U 上的模糊集合扩张原理由下式在 V 上定义一个模糊集合 B：

$$\mu_B(v)=\bigvee_{u\in f^{-1}(v)}(\mu_A(u)) \tag{2.19}$$

即对 $\forall u\in U$，$\mu_B(v)$ 是 $\mu_A(u)$ 的上界，因此，$f(u)=v$，$v\in V$，且设 $f^{-1}(v)$ 非空。当 $f^{-1}(v)$ 对某些 $v\in V$ 为空集时，设 $\mu_B(v)=0$。

2.1.4　隶属函数的建立

隶属函数是模糊集合建立的基石，隶属函数的确定无论理论上或应用上都非常重要，由于造成模糊不确定性的原因是多种多样的，要确定恰当的隶属函数并不容易。在大多数场合下，隶属度无法直接给出，它的建立需要对所描述概念有足够的了解，一定的数学技巧，还包括心理测试的进行与结果的运用等各种因素。正如某一事件的发生与否有一定的不确定性（随机性）一样，某一对象是否符合某一概念也有一定的不确定性。

确定隶属函数的方法很多，最基本的一种就是模糊统计法。根据概率统计的规律，当试验次数足够大时，可以用频率来代替概率。所以，建立隶属函数时，可用隶属频率来代替隶属度。

模糊统计实验有四个要素：①论域U；②U 中的一个元素；③U 中一个边界可变的普通集合 A^*，A^* 联系于一个模糊集合 A 及相应的模糊概念 a；④条件 S，它联系着按模糊概念 a 所进行的划分过程的全部主客观因素，它制约着 A^* 边界的改变。

模糊性产生的根本原因是：S 对概念 a 可能覆盖了被研究的元素 u_0，也可能不覆盖 u_0，这就导致 u_0 对 A^* 的隶属关系不确定。所做的划分引起的 A^* 的变异，可能使模糊统计实验的基本要求是，在每一次实验下，要对 u_0 是否属于 A^* 做一个确切的判断，做 n 次实验，就可算出 u_0 对 A 的隶属频率。

$$u_0 \text{对 } A \text{ 的隶属频率} = \frac{\text{“}u_0 \text{属于 } A^*\text{”的次数}}{n} \tag{2.20}$$

许多实验证明，随 n 的增大，隶属频率呈现稳定性，被称为隶属频率稳定性，频率稳定所在的数值叫做 u_0 对 A 的隶属度。即有：

$$\mu_A(u_0) = \lim_{n\to\infty} \frac{\text{“}u_0 \text{属于 } A^*\text{”的次数}}{n} \tag{2.21}$$

确定隶属函数的方法除此外，其他同样比较实用的确定隶属函数的方法有二元对比排序法、综合加权法、专家确定法、基本概念扩充法及约定俗成的客观尺度法等。二元对比排序法给出了一种先通过事物间的两两对比，确定出其在某种特征下的顺序，而后经过某种处理，以确定事物相对于预定特征的隶属函数或其隶属函数大体形状的方法。人们习惯从两事物的对比中做出它们对某一概念符合程度的判断，但是这种判断往往不满足数学上对“序”的要求，往往不具传递性，而出现循环现象。这往往是由一些模糊概念引起的。但由于在许多情况下，直接给出论域U 中一个模糊集合 A 的隶属度是比较困难的，而比较隶属度的大小是比较容易的，故二元对比排序法在这种情况下具有很大的作用。

综合加权法是对于一个有若干个模糊因素复合而成的模糊概念，可以先求出各个因素的

模糊集的隶属函数，再用综合加权的方法复合出模糊概念的隶属函数。这类问题的实质是通过各组合因素的模糊集的复合来构建总体模糊集的。

专家确定法是专家凭经验给出隶属度的具体数值或采用专家调查法，即带确定度的德尔菲法（利用专家经验与意识，经反馈、调整、分析、提炼，从而得到比较满意的结果）。

基本概念扩充法即在一些基本概念的隶属函数已经确定后，通过对基础隶属函数进行某些运算而得到一些“相关”概念的隶属函数。

另外，有些模糊集所反映的模糊概念已有相应成熟的“指标”，这种“指标”经长期实践验证已成为公认的对客观事物真实而本质的刻画。这样，我们在实际应用中可以根据问题的性质，直接采用这些“指标”作为隶属函数来刻画问题中的不确定性。这种方法就是客观尺度法。在不同的应用下，隶属函数的确定根据试验的结果和目的的侧重点不同而有不同方法，这要视具体的应用情况而定。

2.2 粗糙集经典理论

粗糙集（Rough Set）是波兰科学家 Z.Pawlak 在 20 世纪 80 年代初提出的[6]，经过近 30 年的发展，现已成为一个前沿研究领域。从本质上看，它反映了认知过程在非确定、非模型化信息处理方面的机制和特点，从而成为一种有效的非单调推理工具。其应用范围已拓展至包括机器学习、信号处理、模式识别等较为广泛的领域。它的基本概念是建立在集合结构和语义基础上的，主要有粗糙集、上近似集合（Upper Approximation）、下近似集合（Lower Approximation）和边界区域（Boundary Region）等。

简单地讲，上近似集合是包含与论域概念有关特征的最小意义下的集合；下近似集合是包含与论域概念有关特征的最大意义下的集合；上近似集合中不属于下近似集合的元素所构成的部分属于边界区域。

粗糙集（Rough Set ，RS）理论与方法对于处理复杂系统不失为一种较为有用的方法，因为它与概率方法、模糊集方法、证据理论方法等其他处理不确定性问题理论的显著区别是，它无须提供问题所需处理的数据集合之外的任何先验信息。当然，由于理论未能包含处理不精确或不确定原始数据的机制，所以与其他处理不确定性问题的理论有很强的互补性。粗糙集（Rough Set）理论和模糊集（Fuzzy Set）理论都是针对不确定性问题提出的，它们既相互独立，又相互补充。粗糙集方法与传统的统计及模糊集方法不同的是：后者需要依赖先验知识对不确定性的定量描述，如统计分析中的先验概率、模糊集理论中的模糊度等；而前者只依赖数据内部的知识，用数据之间的近似来表示知识的不确定性。用粗糙集来处理不确定性问题的最大优点在于：它不需要关于数据的预先或附加的信息，而且容易掌握和使用。

粗糙集的一些理论和方法可用来从数据库中发现分类规则。其基本思想是，将数据库中的属性分为条件属性和结论属性，对数据库中的元组根据各个属性不同的属性值分成相应的子集，然后对条件属性划分的子集与结论属性划分的子集之间的上下近似关系生成判定规则。

自 1982 年 Z.Pawlak 提出粗糙集（Rough Set）以来，现已成为一个前沿研究领域。人工智能和其他复杂信息处理通常以分类作为基本机制，粗糙集理论正是建立在分类机制的基础上的，它将分类理解为等价关系，而这些等价关系将论域进行划分。粗糙集理论将划分作为一种描述的手段，而不是最终的目的。由此，粗糙集理论将等价关系对论域的划分与知识等同，或者说将知识理解为对数据的划分。给定一族数据与等价关系 R，在等价关系 R 下对数据集合 U 的划分称为知识。

上近似、下近似、边界区和粗糙隶属函数（Rough Membership Function）是粗糙集的几个重要概念，在下面的内容里将给出详细的解释。

将给定的一个有限的非空集合 U 称为论域，R 为 U 上的一族等效关系。R 将 U 划分为互不相交的基本等价类，二元对 $K=(U,R)$ 构成一个近似空间（Approximation Space）。设 X 为 U 的一个子集，a 为 U 中的一个对象，$[a]_R$ 表示所有与 a 不可分辨的对象所组成的集合，即由 a 决定的等价类。当集合 X 能表示成基本等价类组成的并集时，则称集合 X 是可以精确定义的，否则，集合 X 只能通过近似的方式来刻画。

定义 2.15　集合 X 关于 R 的下近似（Lower Approximation）定义为：

$$R_*(X)=\{a\in U:[a]_R\subseteq X\} \tag{2.22}$$

$R_*(X)$实际上是由那些根据已有知识判断肯定属于 X 的对象所组成的最大的集合，也称为 X 的正区（Positive Region），记做 $\mathrm{POS}(X)$。由根据已有知识判断肯定不属于 X 的对象组成的集合称为 X 的负区（Negative Region）。记做 $\mathrm{NEG}(X)$。

集合 X 关于 R 的上近似（Upper approximation）定义为：

$$R^*(X)=\{a\in U:[a]_R\cap X\neq\phi\} \tag{2.23}$$

$R^*(X)$是所有与 X 相交非空的等价类$[a]_R$的并集，是那些可能属于 X 的对象组成的最小集合。显然，$R^*(X)+\mathrm{NEG}(X)=$论域U。

集合 X 的边界区（Boundary Region）定义为：

$$\mathrm{BN}(X)=R^*(X)-R_*(X) \tag{2.24}$$

$\mathrm{BN}(X)$ 为集合 X 的上近似与下近似之差。如果 $\mathrm{BN}(X)$ 是空集，则称 X 关于 R 是清晰的（Crisp）；反之如果 $\mathrm{BN}(X)$ 不是空集，则称集合 X 为关于 R 的粗糙集（Rough Set）。图 2.1 为粗糙集概念的示意图。下近似、上近似及边界区等概念刻画了一个不能精确定义的集合的近似特性。

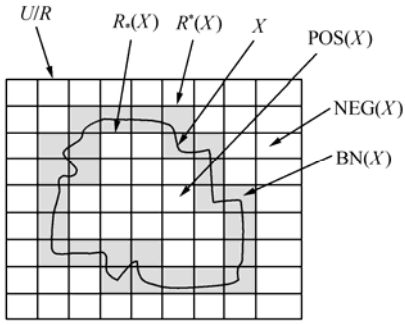


图 2.1 粗糙集概念的示意图

近似精度为：

$$a_R(X)=\frac{|R_*(X)|}{|R^*(X)|} \tag{2.25}$$

其中，$|R(X)|$表示集合 $R(X)$ 的基数或势（Cardinality），对有限集合来说表示集合中所包含元素的个数。显然，$0\leqslant a_R(X)\leqslant 1$。如果 $a_R(X)=1$，则称集合 X 相对于 R 是清晰的；$a_R(X)<1$，则称集合 X 相对于 R 是粗糙的。$a_R(X)$ 可认为是在等价关系 R 下近似集合 X 的精度。

RS 理论中定义了粗糙隶属函数（Rough Membership Function）。通过使用不可分辨关系，定义元素 a 对集合 X 的粗糙隶属函数如下：

$$\mu_x^R=\frac{|X\cap[a]_R|}{|[a]_R|} \tag{2.26}$$

显然 $0\leqslant\mu_x^R\leqslant 1$，粗糙隶属函数也可以用来定义集合 X 的上近似、下近似和边界区。

2.3 知识约简

知识约简是研究近似空间中每个等价关系是否都是必要的，以及如何删除不必要的知识。知识约简在信息系统分析与数据挖掘等领域都具有重要的应用意义。知识之间的依赖性决定知识是否可以进行约简，根据依赖性所定义的知识的重要性往往是知识约简的重要启发式信息。

2.3.1　一般约简[6,7]

在粗糙集理论与应用当中，约简（Reduct）与核（CORE）是两个最重要的概念。直观地，所谓知识的约简是指知识的本质部分，它足以定义所考虑的知识中遇到的所有基本概念，而核是其最重要的部分。

定义 2.16　设 R 是等价关系的一个族集，且设 $r \in R$。若 $\mathrm{IND}(R) = \mathrm{IND}(R - r)$，则称关系 r 在族集 R 中是可缺省的（Dispensable），否则就是不可缺省的（Indispensable）。若族集 R 中的每个关系 r 都是不可缺省的，则族集 R 是独立的（Independent），否则就是依赖的或非独立的。

定义 2.17　若 $Q \subseteq P$ 是独立的，并且 $\mathrm{IND}(Q)=\mathrm{IND}(P)$，则 Q 是关系族集 P 的一个约简（Reduct）。在族集 P 中所有不可缺省的关系的集合称为 P 的核（CORE），以 $\mathrm{CORE}(P)$来表示。

显然，族集 P 有多个约简，约简具有不唯一性。下面的定理是建立约简与核之间联系的重要性质。

定理 2.1　族集 P 的核等于 P 的所有约简的交集。即：

$$\mathrm{CORE}(P) = \bigcap \mathrm{RED}(P) \tag{2.27}$$

其中，$\mathrm{RED}(P)$ 是 P 的所有约简的族集。

从上面的定理可以看出，核的概念具有两方面的意义。首先，可作为计算所有约简的基础，因为核包含于每个约简中，并且其计算是直接的。其次，核可以解释为知识最重要部分的集合，进行知识约简时不能够删除它。

一般产生约简的方法是逐个向核中添加可缺省的关系，并进行检查。注意，可缺省关系集合的幂集的基数是多少，就有多少种添加方式。最好的情况是，所有不可缺省的关系集合本身就是约简，此时约简是唯一的。所以，计算所有约简与计算一个最佳约简（如定义为关系最少）都是 NP 难题。

2.3.2　相对约简

本节将要对约简和核的概念进行进一步的推广，以便使这一理论更具实际操作性。为此，首先需要定义一个分类的正区域的概念。

定义 2.18　设 P 和 Q 是全域 U 上的等价关系的族集，所谓族集 Q 的 P -正区域（P-positive Region of Q），记做 $\mathrm{POS}_P(Q)$，定义为：

$$\mathrm{POS}_P(Q) = \bigcup_{X \in U/Q} P_*(X) \tag{2.28}$$

族集Q的P-正区域是全域U的所有那些使用分类U/P所表达的知识，能够正确地分类与U/Q的等价类之中的对象的集合。一个集合X相对于一个等价关系P的正区域就是这个集合的下近似$P_*(X)$；而一个等价关系Q相对于另一个等价关系P的正区域的概念是解决分类Q的等价类（一般视为决策类）之中的哪些对象可由分类P的等价类（一般视为条件类）来分类的问题。

定义 2.19 设P和Q是全域U上的等价关系的族集，$R \in P$。若：

$$\mathrm{POS}_{\mathrm{IND}(P)}(\mathrm{IND}(Q)) = \mathrm{POS}_{\mathrm{IND}(P-\{R\})}(\mathrm{IND}(Q)) \tag{2.29}$$

则称关系R在族集P中是Q-可省的，否则称为Q-不可省的；如果在族集P中的每个关系R都是Q-不可省的，则称P关于Q是独立的，否则，称为是依赖的。

定义 2.20 $S \subseteq P$称为P的Q-约简（Q-reduct），当且仅当S是P的Q-独立的子族集，且$\mathrm{POS}_s(Q) = \mathrm{POS}_P(Q)$；族集$P$中的所有$Q$-不可省的初等关系的集合，称为族集$P$的$Q$核（$Q$-core），记做$\mathrm{CORE}_Q(P)$。

容易看出，当$P=Q$时，上述定义就是 2.3.1 节所引入的定义。下面的定理是对定理 2.1 的推广。

定理 2.2 族集P的Q-核等于族集P的所有Q-约简的交集。即：

$$\mathrm{CORE}_Q(P) = \bigcap \mathrm{RED}_Q(P) \tag{2.30}$$

其中，$\mathrm{RED}_Q(P)$是族集P的所有Q-约简的族集。

假设P与Q是全域U上的等价关系的族集（知识），族集Q的族集P-正区域$\mathrm{POS}_P(Q)$是使用知识P能够分类于知识Q的概念之中的所有对象的集合。如果整个知识P对于将对象分类于知识Q的概念中都是必要的，那么知识P就是Q-独立的，知识P的Q-核知识是知识P的本质部分，在不影响将对象分类于Q的概念之中的能力的前提下，Q-核知识是不能被删除的。即删除它们的任何部分都将会影响知识P把对象分类于Q的概念之中的能力。知识P的Q-约简是知识P的某种最小子集，它具有与整个知识P相同的把对象分类于知识Q的概念之中的能力。注意，知识P可能有多个约简。在某种意义上，如果知识P仅仅只有一个Q-约简，则知识P是确定的，即把对象分类于知识Q的概念之中时，只有一种使用知识P的方式。当知识P为不确定的，即知识P有多个Q-约简，将对象分类于Q的概念时，一般就有多种使用知识P的方式。若核为空，则这种不确定性就尤其严重。

2.3.3 分辨矩阵[6]

分辨矩阵也是表示知识的一种方法，这种表示有许多有利条件，特别是用它可以解释和便于计算数据核和约简。设$S=(U,A)$是一个信息系统，并设$A=\{a_1,\cdots,a_m\}$，用$\boldsymbol{M}(S)$表示$n\times n$阶矩阵(c_{ij})，称它为S的分辨矩阵，使得：

$$c_{ij}=\{a\in A:a(u_i)\neq a(u_j)\wedge u_i,u_j\in U\wedge i,j=1,\cdots,n\} \tag{2.31}$$

直观地解释，一个输入 c_{ij} 是由所有那些能分辨个体 u_i 和 u_j 的属性组成的。因为 $\boldsymbol{M}(S)$ 是对称的并且对 $i=1,\cdots,n$，$c_{ij}=\phi$，所以我们只利用下三角形部分表示 $\boldsymbol{M}(S)$，即 $1\leqslant j\leqslant i\leqslant n$ 和 $c_{ij}\neq\phi$ 的那部分。

由于任意分辨矩阵 $\boldsymbol{M}(S)$，都可以用下面的方法唯一地确定一个分辨函数 $f_{\boldsymbol{M}(S)}$：一个信息系统的分辨函数拥有 m 个命题变量 $a_1,\cdots,a_m$，其中 $a_i\in A,i=1,\cdots,m$。它的表达形式被定义为全体表达式 $\vee c_{ij}$ 的合取，其中 $\vee c_{ij}$ 是所有 c_{ij} 中元素的析取，其中 $1\leqslant j\leqslant i\leqslant n$，$c_{ij}\neq\phi$。

命题 1　设 $S=(U,A)$ 是一个信息系统，$f_{\boldsymbol{M}(S)}$ 是 S 的一个分辨函数，则该函数的最小简化的析取范式对应于 S 的全体约简。

该命题给出了计算 S 的全体约简的重要方法，即只要将合取范式的分辨函数展开成析取范式，便能得到 S 的全体约简。

命题 2　设 $S=(U,A)$ 是一个信息系统，并且 $B\in\mathrm{RED}(S)$，如果 $A-B\neq\phi$，则 $B\rightarrow_S A-B$。

该命题是说明哪些被约去的属性能从所得到的约简中推导出来，即描述了约简和被约去的属性之间的关系。

命题 3　对每个 $C'\neq\phi\wedge C'\subseteq C$，如果 $B\rightarrow_S C$，则 $B\rightarrow_S C'$，特别地对于每个 $a\in C$，$(B-C)\rightarrow(B-\{a\})$。

该命题揭示了相关的属性集 C，其中的每个属性都是与其前提相关的。

命题 4　设 $B\in\mathrm{RED}(S)$，则约简 B 中的所有属性都是相互独立的，即对任意 $a,a'\in B$，且 $a\neq a'$，既没有 $\{a\}\rightarrow_S\{a'\}$ 成立，也没有 $\{a'\}\rightarrow_S\{a\}$ 成立。

这个命题指出了约简中的每个属性都是独立的，它不与任何属性相关。下面是利用分辨矩阵产生约简的过程：

（1）计算系统 S 的分辨矩阵 $\boldsymbol{M}(S)$；

（2）计算与分辨矩阵相关的分辨函数 $f_{\boldsymbol{M}(S)}$；

（3）计算分辨函数 $f_{\boldsymbol{M}(S)}$ 的最小析取范式，它将给出所有约简。

这个算法的时间与空间的复杂度是关于 S 的大小成指数变化的；当然，它也是在许多实践中更为有效的计算约简的方法。

2.4　决策表的约简

在制定决策的时候是否需要全部的条件属性，能否进行决策表的约简。约简后的决策表具有与约简前的决策表相同的功能，但是约简后的决策表具有更少的条件属性。因此，决策表的约简在工程应用中相当重要，同样的决策表可以通过基于更少量的条件，使我们通过一

些简单的手段就能获得同样要求的结果。严格地说，虽然决策算法和决策表是两个不同的概念，但用决策表表示决策算法比用决策逻辑语言的形式更紧凑，更易于理解，是一种简便的方法，同样，决策算法也可以从逻辑方面来表达决策表，所以两者的有些性质可以相互利用。

2.4.1 决策规则和决策算法[6,7]

在逻辑语言中，含义$\theta \to \psi$称为知识表达语言中的决策规则，θ和ψ分别称为决策规则的前驱和后继，类似于前面所说明的用条件属性和决策属性描述研究对象，它们表达一种因果关系。

当S中决策规则$\theta \to \psi$为真时，我们说该决策规则在S中是一致的，否则说该决策规则在S中是不一致的。当决策规则在S中是一致的时，相同的前驱必导致相同的后继；但同一种后继不一定必须是同一前驱产生的。

当$\theta \to \psi$为一个决策规则，且θ和ψ分别为P基本公式和Q基本公式时，设P、Q已知，则决策规则$\theta \to \psi$称为 PQ 基本决策规则，简称 PQ 规则，这里P、Q属性可以看成前面所说的条件属性和决策属性。

当$\theta_1 \to \psi, \theta_2 \to \psi, \cdots, \theta_n \to \psi$均为基本决策规则时，决策规则$\theta_1 \vee \theta_2 \vee \cdots \vee \theta_n \to \psi$称为基本决策规则$\theta_1 \to \psi, \theta_2 \to \psi, \cdots, \theta_n \to \psi$的组合，简称组合决策规则。

为了考察 PQ 规则是否为真（是否一致或不一致），可以利用下面的命题。

命题 5 当且仅当所有的$\{P \vee Q\}$基本公式在 PQ 规则前驱的$\{P \vee Q\}$规范形式中出现，并且也在 PQ 规则后继的$\{P \vee Q\}$规范形式中出现时，S中 PQ 规则为真（一致的），否则为假（不一致的）。

决策逻辑语言中任何有限决策规则集称为决策逻辑语言中的决策算法，而任何有限基本决策规则称为一个基本决策算法。

当基本决策算法中的所有决策规则都是 PQ 决策规则时，该算法称为 PQ 决策算法，或简称 PQ 算法，记做（P, Q）。当且仅当S中所有决策规则一致时，S中 PQ 算法一致，否则，PQ 算法不一致。

2.4.2 决策规则中的不一致性和不可分辨性

为了检测一个决策算法是否一致，可以利用命题 5，考虑它的全部决策规则是否为真。而下面的命题则给出了一个更为简单的方法。

命题 6 当且仅当对于 PQ 决策算法中任意 PQ 决策规则$\theta_1 \to \psi_1, \theta = \theta_1$，蕴涵$\psi = \psi_1$时，

PQ 决策算法中 PQ 决策规则 $\theta \to \psi$ 是 S 中一致的。

同时我们也注意到，为了检测决策规则 $\theta \to \psi$ 是否为真，必须证明该决策规则的前驱（公式 θ）能够将决策类 ψ 同所讨论的决策算法的其他决策类区分开，这表明“真”这一概念有时也可以被不可区分性的概念代替。显然，若相同的前驱有不同的后继，则这种规则是不一致的。

2.4.3　属性的依赖性

要处理数据，进行决策，就要分析数据的内在联系，讨论属性的依赖性，这里所讨论的属性的依赖性和前面介绍的知识的依赖性是相对应的。当 S 中存在一个一致的 PQ 决策算法时，我们称 S 中属性集 Q 全依赖于（简称依赖）属性集 P，并记做 $P \Rightarrow Q$；当 S 中存在一不一致的 PQ 决策算法时，我们称 S 中属性集 Q 部分依赖于属性集 P。

如前面知识的依赖性的定义，我们也可以利用正区域的概念来定义属性集之间的依赖度。

设（P, Q）为 S 中的一个 PQ 算法，算法中所有一致的 PQ 规则的集合称为算法的正域，记为 $\mathrm{POS}(P,Q)$。决策算法的正域 $\mathrm{POS}(P,Q)$ 是不一致算法的一部分，显然，当且仅当 $\mathrm{POS}(P,Q) \neq (P,Q)$ 或 $\mathrm{card}(\mathrm{POS}(P,Q)) \neq \mathrm{card}(P,Q)$ 时，算法是不一致的。

对于一个 PQ 算法，算法的一致性程度用依赖度 k 来表示，并定义为：

$$k = \mathrm{card}(\mathrm{POS}(P,Q))/\mathrm{card}(P,Q) \tag{2.32}$$

显然，$0 \leqslant k \leqslant 1$。当 $k=1$ 时，算法是一致的；当 $k \neq 1$ 时，算法是不一致的。当 PQ 算法有依赖度 k 时，称属性集 Q 对 P 的依赖度为 k，并记为 $P \Rightarrow_k Q$。

2.4.4　一致决策表的约简

我们知道，利用不可分辨性可以研究知识的约简，即在 S 中存在属性集 $C \subseteq A$，当且仅当 $\mathrm{IND}(A-C) = \mathrm{IND}(A)$ 时 A 是有冗余的，当 $A-C$ 在 A 中冗余且 C 在 S 中是依赖的时，则 C 是 A 的约简。

在这里，讨论的问题将用逻辑方式来表示，并且利用算法的一致性来做出判断和进行约简。

(P,Q) 为一致算法，$a \in P$，在 (P,Q) 算法中，当且仅当 $((P-\{a\}),Q)$ 算法为一致的时，称 (P,Q) 算法中属性 a 是可省的，否则 a 为不可省的。

如果所有的属性 $a \in P$ 在 (P,Q) 算法中是不可省的，则算法 (P,Q) 称为独立的。如果属性子集 $R \subseteq P$，当算法 (P,Q) 是独立且一致的时，R 称为算法 (P,Q) 中 P 的约简。如果属性子集 R 为算法 (P,Q) 中 P 的约简，算法 (R,Q) 称为算法 (P,Q) 的约简，算法的约简是去掉不必要的

条件属性，是对知识表示空间维数进行约简。

算法 (P,Q) 中所有不可省的属性的集合称为算法 (P,Q) 的核，记做 $\mathrm{CORE}(P,Q)$ 。

$$\mathrm{CORE}(P,Q)=\bigcap \mathrm{RED}(P,Q) \tag{2.33}$$

这里，$\mathrm{RED}(P,Q)$ 代表算法 (P,Q) 所有约简的集合。

另外，下面再介绍一下决策表中属性的一些性质。

命题 7 当且仅当 $C \Rightarrow D$ 时，决策表 $T=(U,A,C,D)$ 一致。

通过计算条件属性和决策属性间的依赖程度来检查一致性。当依赖程度等于 1 时，决策表一致，否则不一致。

1．条件属性的约简[7]

为了对决策表进行约简，我们可以采用前面介绍过的分辨矩阵的方法对条件属性进行约简，只不过我们是通过决策属性来得到等价类的，对决策属性相同的个体不予比较。考虑决策表表 2.1，其中条件属性为 a， b， c， d，决策属性为 e，则其对应的分辨矩阵如表 2.2 所示。

表 2.1 决策表

U/A	a	b	c	d	e
u_1	1	0	2	1	0
u_2	0	0	1	2	1
u_3	2	0	2	1	1
u_4	0	0	2	2	2
u_5	1	1	2	1	0

表 2.2 分辨矩阵

U/A	u_1	u_2	u_3	u_4	u_5
u_1					
u_2	a,c,d				
u_3		a,c,d			
u_4	a,d	c	a,d		
u_5		a,b,c,d		a,b,d	

由此分辨矩阵很容易得到核为 $\{c\}$，分辨函数 $f_{\boldsymbol{M}(S)}$ 为 $c\wedge(a\vee d)$，即 $(a\wedge d)\vee(c\wedge d)$，得到两个约简 $\{a,c\}$ 和 $\{c,d\}$。

当讨论的对象与属性的规模较大时，矩阵将占有大量的存储空间。但经过分析，分辨矩阵起到解释的作用，比较直观，其实质是利用逻辑运算中的吸收律和其他演算法则来达到数据约简的目的，所以可省略生成分辨矩阵的中间环节，从表中提取关于属性的逻辑公式。采用基于广义决策逻辑公式演绎算法，也就是利用决策表直接提取逻辑公式，并在逻辑演绎系统下化简该公式，即一边提取那些关于个体是可分辨的属性（决策属性相同的个体不进行比较）并生成公式，一边化简该公式，最后将公式化为析取范式，则每个析取项对应一个约简，达到属性约简的目的。

u_1 与 u_2，u_3，u_4，u_5 关于属性的值是可分辨的分辨合取范式：

$$(a \vee c \vee d) \wedge (a \vee d)$$

经引用吸收律等逻辑运算得到简化式①：$a \wedge d$。

u_2 与 u_3，u_4，u_5 关于属性的值是可分辨的分辨合取范式并上①：

$$(a \vee d) \wedge (a \vee c \vee d) \wedge c \wedge (a \vee b \vee c \vee d)$$

经引用吸收律等逻辑运算得到简化式②：$(a \vee d) \wedge c$。

u_3 与 u_4，u_5 关于属性的值是可分辨的分辨合取范式并上②：

$$(a \vee d) \wedge c \wedge (a \vee d)$$

经引用吸收律等逻辑运算得到简化式③：$(a \vee d) \wedge c$。

u_4 与 u_5 关于属性的值是可分辨的分辨合取范式并上③：

$$(a \vee d) \wedge c \wedge (a \vee b \vee d)$$

经引用吸收律等逻辑运算得到简化式④：$(a \vee d) \wedge c$。

对④式施行 $\wedge$ 对 $\vee$ 的分配律运算，得到如下的分辨吸取范式：$(a \wedge c) \vee (c \wedge d)$。由此得到两个约简：$\{a,c\}$ 和 $\{c,d\}$。

这样表 2.1 就可以简化为如表 2.3 和表 2.4 所示的两个表。

表 2.3　表 2.1 对应的一种简化决策表

U/A	a	c	e
u_1	1	2	0
u_2	0	1	1
u_3	2	2	0
u_4	0	2	2
u_5	1	2	0

表 2.4 表 2.1 对应的一种简化决策表

U/A	c	d	e
u_1	2	1	0
u_2	1	2	1
u_3	2	1	0
u_4	2	2	2
u_5	2	1	0

2．行的约简

对决策表中的重复的行要删除，因为它们的条件属性和决策属性都相同，都表示同一决策规则。另外，决策规则的列表顺序不是本质性的，所以表 2.3 和表 2.4 都可进行约简。例如，表 2.3 可约简为表 2.5。

表 2.5 表 2.3 的约简

U/A	a	c	e
u_1	1	2	0
u_2	0	1	1
u_3	2	2	0
u_4	0	2	2

3．属性的重要性

前面已经提到，约简是粗糙集用于数据分析的重要概念，而所有约简的计算是 NP-hard 问题，因此运用启发信息来简化计算以找出最优或次优约简是必要的。

现在求约简的算法一般都使用核作为计算约简的出发点，来计算一个最好的或者用户指定的最小约简。算法将属性的重要性作为启发规则，按照属性的重要度从大到小逐个加入属性，直到该集合是一个约简为止。各算法对属性重要度的度量不同，目前的报道涉及以下几种度量。

1）根据依赖度的变化来定义

定义 2.21 设 S 为一决策表，C，D 分别为条件属性集和决策属性集。$R \subset C$，对于任意属性 $a \in C - R$ 的重要性定义如下：

$$\mathrm{SGF}(a, R, D) = k(R \bigcup \{a\}, D) - k(R, D) \tag{2.34}$$

其中，$k(R,D)=\text{card}(\text{POS}_R(D))/\text{card}(\text{POS}_C(D))$。

还有一种定义为：

$$\text{SGF}(a,R,D)=\gamma_{R\cup\{a\}}-\gamma_R \tag{2.35}$$

其中，$\gamma_R=\text{card}(\text{POS}_R(D))/\text{card}(U)$。

以上两种定义实质上是相同的，因为当决策表给定后，$\text{card}(\text{POS}_C(D))$和$\text{card}(U)$都是常数，尽管重要性的取值不同，但它们对属性重要性的排序是相同的。

2）根据熵来定义

定义 2.22　设$H(D/R)$为D相对于R的条件熵，属性a的重要性定义如下：

$$\text{SGF}(a,R,D)=H(D/R)-H(D/R\cup\{a\}) \tag{2.36}$$

3）根据在分辨矩阵中出现的频率来定义

设$\boldsymbol{M}$是根据决策表S构造的分辨矩阵，令$p(a)$为在$\boldsymbol{M}$中属性a的属性频率函数，它定义为a在$\boldsymbol{M}$中出现的次数，则：

$$\text{SGF}(a,R,D)=p(a) \tag{2.37}$$

2.4.5　非一致决策表的约简

只有当所有的决策规则都是一致的时，决策表才是一致的，否则决策表是不一致的。对于一致的决策表比较容易处理，在进行约简时，只要判断去掉某个属性或某个属性值时是否会导致不一致规则的产生。而对不一致表进行约简时就不能再使用这种方法了，下面将介绍两种化简不一致表的方法：一种考虑正域的变化，另外一种将不一致表分成完全一致表和完全不一致表两个子表。

不一致决策表约简步骤与一致决策表的约简步骤类似，值得注意的是，前面提到一致决策表的约简步骤，其中有关于重复行的删除，即相同的决策规则可以删除。但在不一致决策表中，这种处理方法将要视决策规则的一致性而定，若决策规则是一致的，则可删除；若是不一致的，则不能删除，下面将具体说明。

1．考虑正域的变化

对于知识表达中不一致的情况，也可以类似一致的情况那样进行决策表的约简，即考虑去掉某些属性后其正域是否发生变化，以判断该属性是否可以去掉。若(P,Q)为不一致算法，$a\in P$，当$\text{POS}(P,Q)=\text{POS}(P-\{a\},Q)$时，$(P,Q)$算法中属性$a$是可省的，否则$a$在$(P,Q)$中是不可省的。

可见一致算法是不一致算法的特殊情况。

而对决策规则约简时，也就是进行条件属性值的约简时，则要分别处理。

若该规则是一致的，首先要计算它的条件属性的核值，即把该行中一个条件属性的值从表中删除，然后看该行中剩下的条件属性的值是否唯一决定此行中的决策属性，若不是，这个值就是核值；求完其条件属性值的核值后，再去求其条件属性值的约简，即将一些条件属性值加入到核值中，得到的各条件属性值能保证决策规则的一致性，并且每个条件属性值都不可省。

若该规则是不一致的，首先要计算它的条件属性的核值，即把该行中一个条件属性的值从表中删除，然后看该行中剩下的条件属性的值所得到的决策属性值的集合与未删除前所得到的决策属性值的集合是否相同，若不是，这个值就是核值；求完其条件属性值的核值后，再去求其条件属性值的约简，即将一些条件属性值加入到核值中，保证得到的决策属性值的集合与原来的决策属性值的集合相同，并且每个条件属性值都不可省。

下面我们举例说明采用这种方法如何对不一致决策表进行约简。

考虑如表 2.6 所示的一个知识表达系统的决策表。

这里，$C=\{a,b,c\}$ 和 $D=\{d,e\}$ 分别为条件属性和决策属性，因为 $U/C=\{\{1,5\},\{2,8\},\{3\},\{4\},\{6\},\{7\}\}$，$U/D=\{\{1\},\{2,7\},\{3,6\},\{4\},\{5,8\}\}$，$\mathrm{POS}_C(D)=\{\{3\},\{4\},\{6\},\{7\}\}$，$\gamma_C(D)=4/8\neq 1$，这表明表 2.6 是不一致的。

表 2.6　一个知识表达系统的决策表

	a	*b*	*c*	*d*	*e*
1	1	0	2	2	0
2	0	1	1	1	2
3	2	0	0	1	1
4	1	1	0	2	2
5	1	0	2	0	1
6	2	2	0	1	1
7	2	1	1	1	2
8	0	1	1	0	1

去掉条件属性 a 后，$U/(C-\{a\})=\{\{1,5\},\{2,7,8\},\{3\},\{4\},\{6\}\}$，$\mathrm{POS}_{C-\{a\}}(D)=\{\{3\},\{4\},\{6\}\}\neq\mathrm{POS}_C(D)$，所以属性 a 是不可省的；去掉条件属性 b 后，$U/(C-\{b\})=\{\{1,5\},\{2,8\},\{3,6\},\{4\},\{7\}\}$，$\mathrm{POS}_{C-\{b\}}(D)=\{\{3\},\{4\},\{6\},\{7\}\}=\mathrm{POS}_C(D)$，所以属性 b 是可省的；去掉属性 c 后，$U/(C-\{c\})=\{\{1,5\},\{2,8\},\{3\},\{4\},\{6\},\{7\}\}$，$\mathrm{POS}_{C-\{c\}}(D)=\{\{3\},\{4\},\{6\}\}=\mathrm{POS}_C(D)$，所以属性 c 是可省的。

由此可得到，表 2.6 的条件属性的核为 a，有两个约简 $\{a,b\}$，$\{a,c\}$。考虑约简 $\{a,b\}$，对应的可以得到表 2.7。

表 2.7　去掉条件属性 c 后的决策表

	a	b	d	e
1	1	0	2	0
2	0	1	1	2
3	2	0	1	1
4	1	1	2	2
5	1	0	0	1
6	2	2	1	1
7	2	1	1	2
8	0	1	0	1

对表 2.7 进行属性值的约简，对于第三条决策规则 $a_2b_0 \to d_1e_1$，它为一致决策规则，其中 a_2，b_0 是核值，因为规则 $a_2 \to d_1e_1$（去掉 b_0）和 $b_0 \to d_1e_1$（去掉 a_2）都为非一致规则。

对于第二条规则 $a_0b_1 \to d_1e_2$，它为不一致规则，其中 a_0 是核值，因为 a_0b_1 对应的决策属性集为 $\{d_1e_2,d_0e_1\}$，去掉 b_1 后，a_0 对应的决策属性集还是 $\{d_1e_2,d_0e_1\}$；而去掉 a_0 后，b_1 对应的决策属性集是 $\{d_1e_2,d_2e_2,d_0e_1\}$，故 a_0 不能去掉。按此种方法计算，表 2.7 中决策规则的所有核值如表 2.8 所示。

表 2.8　表 2.7 中决策规则的所有核值

	a	b	d	e
1	1	0	2	0
2	0	-	1	2
3	2	0	1	1
4	1	1	2	2
5	1	0	0	1
6	-	2	1	1
7	2	1	1	2
8	0	-	0	1

因此，我们得到所有条件属性值的约简表如表 2.9 所示。

表 2.9 所有条件属性值的约简表

	a	b	d	e
1	1	0	2	0
2	0	×	1	2
3	2	0	1	1
4	1	1	2	2
5	1	0	0	1
6	×	2	1	1
7	2	1	1	2
8	0	×	0	1

因此，表 2.9 对应的决策规则为：

$a_1b_0 \rightarrow_{0.5} d_2e_0$； $a_0 \rightarrow_{0.5} d_1e_2$； $a_2b_1 \rightarrow d_1e_2$； $a_2b_0 \vee b_2 \rightarrow d_1e_1$； $a_0 \rightarrow_{0.5} d_0e_1$； $a_1b_1 \rightarrow d_2e_2$；$a_1b_0 \rightarrow_{0.5} d_0e_1$。

2．分成两个子表

命题 8 每个决策表 $T=(U,A,C,D)$ 都可以唯一分解为两个决策表 $T_1=(U_1,A,C,D)$ 和 $T_2=(U_2,A,C,D)$，这样使得表 T_1 中 $C \Rightarrow_1 D$ 和 T_2 中 $C \Rightarrow_0 D$。这里 $U_1=\mathrm{POS}_C(D)$，$U_2=\bigcup \mathrm{BN}_C(X)$，$X \in U/\mathrm{IND}(D)$。

由此命题可见，假设我们已计算出条件属性的依赖度，若表的结果不一致，即依赖度小于 1，则可以将表分解成两个子表：其中的一个表完全不一致，依赖度为 0；另一个表则完全一致，依赖度为 1。当然，只有依赖度大于 0 且不等于 1 时，这一分解才能进行。分解后所得到完全一致的表可按照前面提到的方法进行约简，而对完全不一致的表可不处理，直接生成带粗糙算子的决策规则。

决策表的约简步骤如下：

（1）对决策表进行条件属性的约简，即从决策表中消去某一列；

（2）消去重复的行；

（3）消去每一决策规则中属性的冗余值。

应该注意到，与知识表达系统的一般表达相比，这里的行不表示对任何实际对象的描述，因此重复行表示的是同样的决策，所以可以把它消去。

约简后的决策表是一个不完全的决策表，它仅含那些在决策时所必需的条件属性值，但它具有原始知识表达系统的所有知识。

表 2.6 可分解为如下的两个子表，如表 2.10 和表 2.11 所示。

表 2.10　完全一致的决策表

	a	*b*	*c*	*d*	*e*
3	2	0	0	1	1
4	1	1	0	2	2
6	2	2	0	1	1
7	2	1	1	1	2

表 2.11　完全不一致的决策表

	a	*b*	*c*	*d*	*e*
1	1	0	2	2	0
2	0	1	1	1	2
5	1	0	2	0	1
8	0	1	1	0	1

对于表 2.10，$U/C=\{\{3\},\{4\},\{6\},\{7\}\}$，$U/D=\{\{3,6\},\{4\},\{7\}\}$，$\mathrm{POS}_C(D)=\{\{3\},\{4\},\{6\},\{7\}\}$，$\gamma_C=4/4=1$。因此表 2.10 是完全一致的，该表中所有的决策规则是一致的。

对于表 2.10 我们采用前面所提到的方法进行约简，得到它对应的条件属性的约简为 $\{a,b\}$、$\{a,c\}$和$\{b,c\}$。取约简$\{a,b\}$，对应的表如表 2.12 所示。

表 2.12　去掉条件属性 *c* 的决策表

	a	*b*	*d*	*e*
3	2	0	1	1
4	1	1	2	2
6	2	2	1	1
7	2	1	1	2

对表 2.12 进行条件属性值的约简，得到其对应的决策规则集为：$b_0 \vee b_2 \to d_1e_1$；$a_1 \to d_2e_2$；$a_2b_1 \to d_1e_2$。

对表 2.11 不进行处理，直接生成带粗糙算子的决策规则集为：$a_1b_0c_2 \to_{0.5} d_2e_0$；$a_0b_1c_1 \to_{0.5} d_1e_2$；$a_1b_0c_2 \to_{0.5} d_0e_1$；$a_0b_1c_1 \to_{0.5} d_0e_1$。

最后，将所有的对应于完全一致决策表的决策规则与对应于完全不一致决策表的决策规则合并，就得到了对应于原来的不一致决策表的决策规则。

2.5 基于属性值的约简算法

2.5.1 什么是属性值的约简[7]

正如前面所述，粗糙集中决策表的化简一般都要用到属性约简，但就某一具体的规则而言，属性约简就等价于其值的约简。对决策表而言，属性值的约简就是决策规则的约简。决策规则的约简是利用决策逻辑分别通过消去决策规则集中每条决策规则的不必要条件来实现的，它不是整体上约简属性，而是针对每条决策规则，去掉表达该规则时的冗余属性值，以便进一步使决策规则最小化。

已经知道，决策规则的约简就是利用决策逻辑消去决策规则集中每个决策规则的不必要条件，即计算规则集中每个决策规则的核和约简。

对决策表进行属性值的约简，也就是决策规则的约简，实际上是针对条件属性而言的。而每一行都对应一条决策规则，所以要计算某决策规则的条件属性的核值，可先把该行中的一个条件属性的值从表中删去，然后看剩下的该行中条件属性的值是否唯一决定此行中的决策属性，若不是，这个值就是核值；求完某决策规则的条件属性的核值后，再去求它的条件属性值的约简，即将一些条件属性值加入到核值中，得到的各条件属性值能保证表的一致性，并且每个条件属性值都不可省。若在决策表的约简表中也出现了重复行，也应该将其删除，因为它们还是表示相同的决策规则。

以表 2.5 为例，在第一条决策规则 $a_1c_2 \rightarrow e_0$ 中，其中 a_1 是核值，因为 $a_1 \rightarrow e_0$（去掉 c_2）为真，而 $c_2 \rightarrow e_0$（去掉 a_1）为假，故不能去掉 a_1。按此种方法计算，表 2.5 中每一个决策规则的所有核值如表 2.13 所示。

表 2.13 表 2.5 中有一个决策规则的所有核值

U/A	*a*	*c*	*e*
u_1	1	-	0
u_2	-	1	1
u_3	2	-	0
u_4	0	2	2

求完所有的核值后，再求每一决策规则的约简。如第一条决策规则有一个约简：$a_1 \rightarrow e_0$，

因为这个决策规则能保持表的一致性。如此可求得表 2.5 的约简表，如表 2.14 所示。

表 2.14　表 2.5 的约简表

U/A	a	c	e
u_1	1	×	0
u_2	×	1	1
u_3	2	×	0
u_4	0	2	2

该决策表的决策规则集为：$a_1 \vee a_2 \rightarrow e_0$；$c_1 \rightarrow e_1$；$a_0 c_2 \rightarrow e_2$。

2.5.2　属性值的约简在决策表当中的应用

对数据进行分析和推理，从中发现隐含的知识，揭示潜在的规律，是粗糙集的一个重要任务，近年来人们对粗糙集研究大致可以分为两个方面：一是理论研究；二是应用研究。而理论研究主要集中在属性的约简算法上，就寻求一般的完备约简而言，好多算法是很有效的，如参考文献[8]、[9]。但这些算法都是沿着传统的粗糙集理论思路发展的，即把全部或者绝大多数的精力和时间集中到寻找能够表示整个决策表的最小属性集上。然而，正如我们前面所介绍的一样，这只是针对全局的一个粗加工，从 2.5.1 节可以看出，就具体的一条规则而言，它就等价于属性值的约简，为此，我们提出了一种用属性值的约简直接得到规则的算法，使约简过程更加直接，其意义也更加直观。

1．类的相对约简

为了能够说明问题，我们首先就前面已经提到的相对约简的问题，再次对它进行一下新的认识和定义。

1）类的约简

设族集 $F=\{X_1, X_2, \cdots, X_n\}$，其中 $X_i \subseteq U$。

定义 2.23　若 $\bigcap(F-\{X_i\})=\bigcap F$，则 X_i 是可缺省的，否则 X_i 就是不可缺省的。

定义 2.24　若族集 F 中所有的部分都是不可缺省的，则称 F 是独立的，否则，称 F 是依赖的。

定义 2.25　若存在族集 $H \subseteq F$，且 H 是独立的；$\bigcap H=\bigcap F$，则称 H 是 F 的一个约简。

其中，$\bigcap F = X_1 \bigcap X_2 \bigcap \cdots \bigcap X_n$，$X_i$ 表示第 i 类，U 是全域。

2）类的相对约简

定义 2.26 给定族集 $F=\{X_1,X_2,\cdots,X_n\}$，其中 $X_i\subseteq U$，若存在 $Y\subseteq F$，使得 $\bigcap F\subseteq Y$，且 $\bigcap(F-\{X_i\})\subseteq Y$，则称 X_i 在 $\bigcap F$ 中是关于 Y 可缺省的，记做 Y-dispensable；否则，称 X_i 在 $\bigcap F$ 中是关于 Y 不可缺省的，记做 Y-indispensable。

定义 2.27 若族集 F 中所有的部分在 $\bigcap F$ 中都是不可缺省的，则称 F 是关于 Y 独立的，记做 Y-independent；否则，称 F 在 $\bigcap F$ 中是关于 Y 依赖的，记做 Y-dependent。

定义 2.28 若存在族集 $H\subseteq F$，且 H 在 $\bigcap F$ 中是 Y-independent 的；$\bigcap H\subseteq Y$，则称 H 是 $\bigcap F$ 中的一个相对约简，记做 Y-reduct。$\bigcap F$ 中所有的 Y-indispensable 的集合称做 $\bigcap F$ 的相对于 Y 的核，记做 Y-core。

其中，$\bigcap F=X_1\bigcap X_2\bigcap\cdots\bigcap X_n$，$X_i$ 表示第 i 类，U 是全域。

2．对决策表的进一步认识[10]

简单地讲，一个知识表达系统的决策表是这样一个二维表，它的每一列表示一个属性及其相应的取值；每一行表示一个实在的对象。而决策表就是把属性区分为条件属性和决策属性两类，而把每一行看做是一条决策规则的这样一个知识表达系统。

表 2.15 是某商场对各类人群是否购买计算机的情况统计表。

表 2.15 某商场对各类人群是否购买计算机的情况统计表

	Age	Income	Student	Credit_rating	Class:buys_computer
x_1	≤30	high	no	fair	no
x_2	≤30	high	no	excellent	no
x_3	31…40	high	no	fair	yes
x_4	>40	medium	no	fair	yes
x_5	>40	low	yes	fair	yes
x_6	>40	low	yes	excellent	no
x_7	31…40	low	yes	excellent	yes
x_8	≤30	medium	no	fair	no
x_9	≤30	low	yes	fair	yes
x_{10}	>40	medium	yes	fair	yes
x_{11}	≤30	medium	yes	excellent	yes
x_{12}	31…40	medium	no	excellent	yes
x_{13}	31…40	high	yes	fair	yes
x_{14}	>40	medium	no	excellent	no

表 2.15 中 Age、Income、Student 和 Credit_rating 是条件属性， Class:buys_computer 是决策属性。注意，到底属性中哪些是条件属性，哪些是决策属性要视具体的情况而定，一般来讲解决问题的目的决定了决策属性。另外需要注意，这里表 2.15（将它视为一个决策表）中的 x_i 仅仅是第 i 条规则的一个表示符。

设决策表 T 表示为：$T=(U,A,C,D)$。其中，U 表示全域，A 表示属性集，C 和 D 是 A 的两个子集，分别表示条件属性集和决策属性集。对于属性 A，它有一个属性值域 V，用 V_a 来代表属性 a 的值，在上例中 V_a={(≤30),(31…40),(>40)}。为了简单起见，让我们分别用 1，2 和 3 来代表 V_a 中的(≤30)， (31…40) 和 (>40)；其余属性可以类推。这样我们就可以将表 2.15 简单地表示为表 2.16。

表 2.16　简化后的表 2.15

	Age	Income	Student	Credit_rating	Class:buys_computer
x_1	1	3	2	1	2
x_2	1	3	2	2	2
x_3	2	3	2	1	1
x_4	3	2	2	1	1
x_5	3	1	1	1	1
x_6	3	1	1	2	2
x_7	2	1	1	2	1
x_8	1	2	2	1	2
x_9	1	1	1	1	1
x_{10}	3	2	1	1	1
x_{11}	1	2	1	2	1
x_{12}	2	2	2	2	1
x_{13}	2	3	1	1	1
x_{14}	3	2	2	2	2

这里 $C=\{\text{Age,Income,Student,Credit\_rating}\}$， $D=\{\text{Class:buys\_computer}\}$， $V=\{1,2,3\}$。因为在实际应用中，我们总希望能够用最少的条件属性表示一条规则。这就需要对决策表进行化简。而决策表的化简一般为三个步骤：列删除，即条件属性的约简；重复行的删除，即重复规则的合并；属性值的删除。其中，属性值的删除是最难处理的。不难验证，表 2.16 中条件属性相对于决策属性的约简就是它本身。经计算得：

$$\text{POS}_C(D)=U$$

$$\mathrm{POS}_{C-\{\mathrm{Age}\}}(D)=\{x_2,x_5,x_9,x_{10},x_{11},x_{12},x_{13},x_{14}\}\neq \mathrm{POS}_C(D)$$
$$\mathrm{POS}_{C-\{\mathrm{Income}\}}(D)=U=\mathrm{POS}_C(D)$$
$$\mathrm{POS}_{C-\{\mathrm{Student}\}}(D)=U=\mathrm{POS}_C(D)$$
$$\mathrm{POS}_{C-\{\mathrm{Credit\_rating}\}}(D)=\{x_1,x_2,x_3,x_7,x_8,x_9,x_{10},x_{11},x_{12},x_{13}\}\neq \mathrm{POS}_C(D)$$

所以，{Age,Credit_rating} 是属性集 C 的 D-core，{Age,Credit_rating,Income} 和 {Age,Credit_rating,Student} 是属性集 C 的两个 D-reduct，而 Income 和 Student 都是 D-dispensable 的。到这里我们就可以从决策表中删除 Income 或 Student 所在的列，但为了验证属性值约简的有效性，不妨暂时先不要删除。

2.5.3 属性值的直接约简及应用

若 B 是一个属性集，用 $[x]_B$ 表示关于 B 的划分的族集中，x 所在的那个集合。可以解释如下。

设 $U/\mathrm{IND}(B)=\{X_1,X_2,\cdots,X_n\}$，$x\in X_i$，则 $[x]_B=X_i$；它表示一个类，B 中各个属性的值就是这个类区别于其他类的特征。

若 $a\in B$，用 $a(x)$ 来表示属性 a 在对象 x 上的取值。则可用 $[x]_a$ 来表示 $U/\mathrm{IND}(a)$ 中所有 a 的取值等于 $a(x)$ 的对象的集合，如表 2.16 中 $\mathrm{Age}(x_1)=1$，而 $[x_1]_{\mathrm{Age}}=\{x_1,x_2,x_8,x_9,x_{11}\}$，那么 $[x]_B=\bigcap_{a\in B}[x]_a$。显然，就针对某一具体的规则 x 而言，a 可以看做和 $a(x)$ 是一回事，因为在一条规则中一个属性只有一个确定的值。例如，在表 2.16 的第一条规则中如果去掉属性 Age，也就相当于去掉了其值 $\mathrm{Age}(x_1)=1$。因此，某一具体的规则的条件属性约简实际上就是它的条件属性值的约简，它的属性约简和属性核分别是其值约简和值核，属性值的约简由此而来。那么属性值的约简方法就和属性的约简完全一样了。根据定义 2.8，为了寻找不可缺省的类，我们必须一次删除一个类，然后检查它们的交集是否仍然包含在对应的决策类里面。

就以表 2.16 为例，为了书写方便我们在这里用 a,i,s,c 和 b 来分别代替 Age，Income，Student，Credit_rating 和 Class:buys_computer（如用 $[x]_a$ 代替 $[x]_{\mathrm{Age}}$）。就如前面所讲的，我们知道属性值的约简是针对每一具体的决策规则而言的，为了说明这个问题，让我们来计算一下表 2.16 中第三条规则的条件属性的值核，即族集 $F=\{[x_3]_a,[x_3]_i,[x_3]_s,[x_3]_c\}$ 的核。

$[x_3]_C=[x_3]_a\bigcap[x_3]_i\bigcap[x_3]_s\bigcap[x_3]_c=\{x_3,x_7,x_{12},x_{13}\}\bigcap\{x_1,x_2,x_3,x_{13}\}\bigcap\{x_1,x_2,x_3,x_4,x_8,x_{12},x_{14}\}\bigcap\{x_1,x_3,x_4,x_5,x_8,x_9,x_{10},x_{13}\}=\{x_3\}$，而且 $a(x_3)=2$，$i(x_3)=3$，$s(x_3)=2$ 和 $c(x_3)=1$，下面我们逐一删去 $[x_3]_a$，$[x_3]_i$，$[x_3]_s$ 和 $[x_3]_c$ 来看它们的剩余类的交集是否包含在决策类 $[x_3]_D=\{x_3,x_4,x_5,x_7,x_9,x_{10},x_{11},x_{12},x_{13}\}$ 中，即：

$$[x_3]_{C-\{a\}}=[x_3]_i\bigcap[x_3]_s[x_3]_c=\{x_1,x_3\}\subset[x_3]_D$$
$$[x_3]_{C-\{i\}}=[x_3]_a\bigcap[x_3]_s\bigcap[x_3]_c=\{x_3\}\subseteq[x_3]_D$$

$$[x_3]_{C-\{s\}} = [x_3]_a \cap [x_3]_i \cap [x_3]_c = \{x_3, x_{13}\} \subseteq [x_3]_D$$
$$[x_3]_{C-\{c\}} = [x_3]_a \cap [x_3]_s \cap [x_3]_i = \{x_3\} \subseteq [x_3]_D$$

所以 x_3 的核值是 $a(x_3)=2$，用同样的方法我们可以计算出表中其余各决策规则的条件属性的核值，如表 2.17 所示。

表 2.17　表 2.16 中各决策规则的条件属性的核值

	Age	Income	Student	Credit_rating	Class:buys_computer
x_1	-	-	-	-	2
x_2	-	-	-	-	2
x_3	2	-	-	-	1
x_4	3	-	-	1	1
x_5	-	-	-	1	1
x_6	3	-	-	2	2
x_7	2	-	-	-	1
X_8	1	-	-	-	2
x_9	-	-	-	-	1
x_{10}	-	-	-	-	1
x_{11}	-	-	-	-	1
x_{12}	2	-	-	-	1
x_{13}	-	-	-	-	1
x_{14}	3	-	-	2	2

从表 2.17 可以看出显然 Income 和 Student 是 *D*-dispensable 的，这和前面用属性约简的方法得到的结果是一样的。这也证明了属性值的约简是有效的。

经计算可知（删除 Income ）：

x_1 的 *D*-reduct 有 $\{a,s\}$ 一个；

x_2 的 *D*-reduct 有 $\{a,s\}$ 一个；

x_3 的 *D*-reduct 有 $\{a\}$、$\{a,s\}$ 和 $\{a,c\}$ 三个；

x_4 的 *D*-reduct 有 $\{a,c\}$ 一个；

x_5 的 *D*-reduct 有 $\{a,c\}$ 和 $\{s,c\}$ 两个；

x_6 的 *D*-reduct 有 $\{a,c\}$ 一个；

x_7 的 *D*-reduct 有 $\{a,s\}$ 和 $\{a,c\}$ 两个；

x_8 的 *D*-reduct 有 $\{a,s\}$ 和 $\{a,c\}$ 两个；

x_9 的 D-reduct 有 $\{a,s\}$ 和 $\{s,c\}$ 两个；

x_{10} 的 D-reduct 有 $\{a,s\}$ 和 $\{s,c\}$ 两个；

x_{11} 的 D-reduct 有 $\{a,s\}$ 和 $\{a,c\}$ 两个；

x_{12} 的 D-reduct 有 $\{a\}$、$\{a,s\}$ 和 $\{s,c\}$ 三个；

x_{13} 的 D-reduct 有 $\{a\}$、$\{a,s\}$、$\{a,c\}$ 和 $\{s,c\}$ 四个；

x_{14} 的 D-reduct 有 $\{a,c\}$ 一个。

那么理论上可以得出 $3^2\times4\times2^6$ 种方案。任选其中的一个如表 2.18 所示。

表 2.18 方案之一

	Age	Student	Credit_rating	Class:buys_computer
x_1	1	2	-	2
x_2	1	2	-	2
x_3	2	-	-	1
x_4	3	-	1	1
x_5	3	-	1	1
x_6	3	-	2	2
x_7	2	-	-	1
x_8	1	-	1	2
x_9	1	1	-	1
x_{10}	3	-	1	1
x_{11}	1	1	-	1
x_{12}	2	-	-	1
x_{13}	2	-	-	1
x_{14}	3	-	2	2

下面将 Income 所在的列删除，合并重复的规则得表 2.19。

表 2.19 删除 Income 合并重复的规则后的结果

	Age	Student	Credit_rating	Class:buys_computer
x_1	1	2	-	2
x_2	1	1	-	1
x_3	2	-	-	1
x_4	3	-	2	2

续表

	Age	Student	Credit_rating	Class:buys_computer
x_5	3	-	1	1
x_6	1	-	1	2

表 2.19 和表 2.16 是一致的，但显然表 2.19 要简单得多。可见属性值的约简在决策表的化简中是非常重要且有效的。而且，我们可以直接用属性值的约简去化简决策表而不必先去做属性约简。

2.6　粗糙集的扩展模型

基本的 RS 模型在应用于实际数据分析时，经常会遇到噪声、数据缺失等一系列问题，因此，出现了许多基本 RS 理论的扩展模型，其中典型的有变精度粗糙集模型、概率粗糙集模型等。在数据集存在噪声等干扰情况下，基本 RS 模型会由于对数据的过拟合使其对新数据的预测或分类能力大为降低。为增加粗糙集模型的抗干扰能力，Ziarko 提出了变精度粗糙集模型，通过引入一个误差精度，使其具有一定的容错性。基本 RS 模型是基于严格的确定性知识，忽视了可利用信息的不确定性，对一些相互矛盾的知识无能为力。因此，概率粗糙集通过引入信息论与概率测度等描述知识的不确定性，从概率的角度对具有矛盾的知识进行处理和刻画，弥补了基本 RS 模型的不足。

2.6.1　可变精度粗糙集模型

粗糙集理论的中心问题是分类分析，基本 RS 理论的一个局限性是它所处理的分类是完全正确的或是肯定的，因此必须严格按等价类来分类，即“包含”或“不包含”，并没有某种程度上的包含，当应用到更加广泛的对象数据集的诊断时，无法保证较高的正确诊断率。因此引入变精度粗糙集模型应用于故障诊断系统，它是在基本 RS 模型的基础上引入 β（$0 \leqslant \beta \leqslant 0.5$）来刻画数据的不一致，允许一定程度的错误分类率存在。变精度粗糙集模型（简称 VPRS 模型）的引入有利于用粗糙集理论从认为不相关的数据中发现相关的数据。当 $\beta=0$ 时，VPRS 模型就是基本 RS 模型。变精度粗糙集模型的相关理论[11]如下。

1）相对错误分类率

设 X，Y 表示有限论域 U 的非空子集，定义相对错误分类率为：

$$c(X,Y)=\begin{cases}1-|X\cap Y|/|X|, & |X|>0\\ 0, & |X|=0\end{cases} \tag{2.38}$$

相对错误分类率表示将集合 X 中的元素分到集合 Y 中所产生的错误分类的比例。

2）多数包含关系

在基本 RS 模型中，是严格按照等价类来分类的，是“包含”或“不包含”的关系。设 X，Y 表示有限论域 U 的非空子集，如果对于 $\forall x\in X$，有 $x\in Y$ 则称 Y 包含 X，记做 $Y\supseteq X$；而在变精度粗糙集模型中，对应于标准包含关系，引入了多数包含关系，定义为：

$$Y\overset{\beta}{\supseteq}X \Leftrightarrow c(X,Y)\leqslant\beta \tag{2.39}$$

“多数”要求 X 和 Y 中的公共元素的数目大于 X 中元素数目的 50%。

3）VPRS 模型中的近似集

类似于基本 RS 模型，可定义近似空间上关于分类误差 β 的粗糙上、下近似等相关概念。

设 (U,R) 为近似空间，其中 U 为非空有限集合，R 是 U 上的一个等价关系，$U/R=\{E_1,E_2,\cdots,E_n\}$ 表示 R 产生的等价类。对于 $X\subseteq U$，X 的 β 下近似为：

$$\underline{R}_\beta X=\bigcup\{E\in U/R\mid X\overset{\beta}{\supseteq}E\} \tag{2.40}$$

或者，

$$\underline{R}_\beta X=\bigcup\{E\in U/R\mid c(E,X)\leqslant\beta\} \tag{2.41}$$

$\underline{R}_\beta X$ 也称为正区域，记为 $\mathrm{POSR}_\beta(X)$。

X 的 β 上近似为：

$$\overline{R}_\beta X=\bigcup\{E\in U/R\mid c(E,X)<1-\beta\} \tag{2.42}$$

X 的 β 边界域为：

$$\mathrm{BNR}_\beta(X)=\bigcup\{E\in U/R\mid \beta<c(E,X)<1-\beta\} \tag{2.43}$$

X 的 β 负区域为：

$$\mathrm{NEGR}_\beta(X)=\bigcup\{E\in U/R\mid c(E,X)\geqslant 1-\beta\} \tag{2.44}$$

X 的 β 正区域可理解为将 U 中的对象以不大于 β 的分类误差分于 X 的集合；X 的 β 负区域理解为将 U 中的对象以不大于 β 的分类误差分于 X 的补集的集合。

4）VPRS 模型中分类能力的刻画

β 精度为：

$$\alpha(R,\beta,X)=|\underline{R}_\beta X|/|\overline{R}_\beta X| \tag{2.45}$$

β 越大，相对精度将越大。

设 $S=(U,A,V,f)$ 是一个信息系统，$C\cup D=A$，C、D 分别为条件属性和决策属性。定

义β 依赖性为：

$$\gamma(C,D,\beta)=|\mathrm{POS}(C,D,\beta)|/|U| \tag{2.46}$$

其中，

$$|\mathrm{POS}(C,D,\beta)|=|\bigcup_{Y\in U/D}\underline{\mathrm{IND}(C)}_{\beta}Y| \tag{2.47}$$

它描述了系统对执行具有分类误差的对象分类质量性能的好坏。

2.6.2　概率粗糙集模型

在实际应用中，基本 RS 模型是基于确定性知识库的，它的近似空间是完全确定的，它对一些局部不能正确分类却可以对大部分数据进行准确分类的规则无法处理，对于不协调的故障模式规则的提取显得无能为力。变精度粗糙集模型虽然可以实现在整体上较优的信息处理能力，但对具有矛盾的诊断规则的处理则过于粗糙化，由于实际系统中各种故障模式的出现具有随机性，且对于不协调的故障模式将其归于不同故障类别的后果一般也是不同的，因此本节将从概率论的观点出发，引入概率粗糙集（简称 PRS）模型，并基于贝叶斯决策理论对不相容的故障模式规则加以分析。

1．概率测度及信息熵[12]

在信息论中，X 称为信息源。对于一个给定的信息源，随着试验次数的增加，信息源的信息量会逐渐减少。我们用信息熵作为对信息源的不确定性的度量。有如下几个定义。

定义 2.29　设U 是论域，X_1，X_2，…，X_n是U 的一个划分，称

$$H(X)=-\sum_{i=1}^{n}p_i\log p_i \tag{2.48}$$

为信息源 X 的信息熵。这里信息源可以认为是条件属性集C或是决策属性集D，对应于故障特征属性集C或是故障种类集D。当对数的底取 2 时，单位为比特（bit）；当以自然数 e 为底时，单位为奈特（nat）；当以 10 为底时，单位为哈特（hart）。

定义 2.30　设

$$Y=\begin{Bmatrix}Y_1,Y_2,\cdots,Y_n\\ q_1,q_2,\cdots q_n\end{Bmatrix} \tag{2.49}$$

是另一个信息源，即$Y_1,Y_2,\cdots,Y_n$是U 的另一划分，q_i是与 Y_i相对应的概率，则已知信息源 X 时信息源Y 的条件熵为：

$$H(Y \mid X)=\sum_{i=1}^{k} H(Y \mid X_i)P(X_i) \tag{2.50}$$

其中，

$$H(Y \mid X_i)=-\sum_{i=1}^{k} P(Y_j \mid X_i)P(Y_i \mid X_i) \tag{2.51}$$

为事件 X_i 发生时信息源 Y 的条件熵。

定义 2.31 信息源 X 和 Y 的互信息量为：

$$I(X;Y)=H(X)-H(X \mid Y) \tag{2.52}$$

它反映了一个信息源从另一个信息源获取的信息量。互信息量是对称的，即：

$$\begin{aligned} I(X;Y) &= H(X)-H(X \mid Y) \\ &= H(Y)-H(Y \mid X)=I(Y;X) \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} P(X_i \cap Y_j)\log\frac{P(Y_j \mid X_i)}{P(Y_j)} \\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} P(X_i \cap Y_j)\log\frac{P(X_i \mid Y_j)}{P(X_i)} \end{aligned} \tag{2.53}$$

与定义 2.29 一样，这里对数的底不同则对应的单位也不同。

2．概率粗糙集模型

设 U 是有限对象构成的论域，R 是 U 上的等价关系，令 P 为定义在 U 的子集类构成的 σ 代数上的概率测度，$A_p=(U,R,P)$ 称为概率近似空间。U 中的每个子集称为概念，它代表一个随机事件。$P(X \mid Y)$ 表示事件 Y 发生下 X 出现的条件概率，也可解释为随机选择的对象在概念 Y 的描述下属于 X 的概率。概率粗糙集模型有四类，分别如下。

（1）设 $0 \leqslant \beta \leqslant \alpha \leqslant 1$，对于任意的 $X \subseteq U$，定义 X 关于概率近似空间 A_p 依参数 α、β 的概率（Ⅰ）型下近似 $\underline{\mathrm{PI}}_{\alpha}(X)$ 和上近似 $\overline{\mathrm{PI}}_{\beta}(X)$ 如下：

$$\underline{\mathrm{PI}}_{\alpha}(X)=\{x \in U \mid P(X \mid [x]) \geqslant \alpha\} \tag{2.54}$$

$$\overline{\mathrm{PI}}_{\beta}(X)=\{x \in U \mid P(X \mid [x]) > \beta\} \tag{2.55}$$

X 关于 A_p 依参数 α、β 的概率（Ⅰ）型的正域、边界域和负域分别为：

$$\mathrm{POS}(X,\alpha,\beta)=\underline{\mathrm{PI}}_{\alpha}(X)=\{x \in U \mid P(X \mid [x]) \geqslant \alpha\} \tag{2.56}$$

$$\mathrm{BN}(X,\alpha,\beta)=\{x \in U \mid \beta < P(X \mid [x]) < \alpha\} \tag{2.57}$$

$$\mathrm{NEG}(X,\alpha,\beta)=U \setminus \overline{\mathrm{PI}}_{\beta}(X)=\{x \in U \mid P(X \mid [x]) \leqslant \beta\} \tag{2.58}$$

正域随着 α 的减小而增大，负域则随着 β 的增大而增大，同时边界域减小。

特别地当 $\alpha=1$，$\beta=0$ 时，若取

$$P(X\,|\,[x])=\frac{|X\cap[x]|}{|[x]|} \tag{2.59}$$

则概率（Ⅰ）型下近似 $\underline{\mathrm{PI}}_{\alpha}(X)$ 和上近似 $\overline{\mathrm{PI}}_{\beta}(X)$ 即为基本 RS 模型下的上、下近似。

由上面的定义可以看出，$\underline{R}(X)\subseteq\underline{\mathrm{PI}}_{\alpha}(X)\subseteq\overline{\mathrm{PI}}_{\beta}(X)\subseteq\overline{R}(X)$。因此，概率（Ⅰ）型的边界域比相应的基本 RS 模型的边界域小，而正域和负域都比较大，它的应用范围比基本 RS 模型更加广泛。

（2）设 $0\leqslant\beta<\alpha<1$，对于任意的 $X\subseteq U$，定义 X 关于概率近似空间 A_p 依参数 α、β 的概率（Ⅱ）型下近似 $\underline{\mathrm{PII}}_{\alpha}(X)$ 和上近似 $\overline{\mathrm{PII}}_{\beta}(X)$：

$$\underline{\mathrm{PII}}_{\alpha}(X)=\{x\in U\,|\,P(X\,|\,[x])>\alpha\} \tag{2.60}$$

$$\overline{\mathrm{PII}}_{\beta}(X)=\{x\in U\,|\,P(X\,|\,[x])\geqslant\beta\} \tag{2.61}$$

这里介绍的概率粗糙集模型（Ⅱ）与（Ⅰ）是基于同一个概率近似空间的，表面上差别不大，但不能相互替代。

（3）设 $0\leqslant\beta<\alpha<1$，对于任意的 $X\subseteq U$，定义 X 关于概率近似空间 A_p 依参数 α、β 的概率（Ⅲ）型下近似 $\underline{\mathrm{PIII}}_{\alpha}(X)$ 和上近似 $\overline{\mathrm{PIII}}_{\beta}(X)$：

$$\underline{\mathrm{PIII}}_{\alpha}(X)=\{x\in U\,|\,P(X\,|\,[x])>\alpha\} \tag{2.62}$$

$$\overline{\mathrm{PIII}}_{\beta}(X)=\{x\in U\,|\,P(X\,|\,[x])>\beta\} \tag{2.63}$$

（4）设 $0\leqslant\beta<\alpha<1$，对于任意的 $X\subseteq U$，定义 X 关于概率近似空间 A_p 依参数 α、β 的概率（Ⅳ）型下近似 $\underline{\mathrm{PIV}}_{\alpha}(X)$ 和上近似 $\overline{\mathrm{PIV}}_{\beta}(X)$ 如下：

$$\underline{\mathrm{PIV}}_{\alpha}(X)=\{x\in U\,|\,P(X\,|\,[x])\geqslant\alpha\} \tag{2.64}$$

$$\overline{\mathrm{PIV}}_{\beta}(X)=\{x\in U\,|\,P(X\,|\,[x])\geqslant\beta\} \tag{2.65}$$

2.7　小结

模糊集理论是 1965 年被提出来的。经典的模糊集模型从隶属函数出发定义模糊集，从而建立模糊集理论和方法。隶属函数往往依靠专家的经验知识，以先验知识为基础。事实上，正因为建立在可靠的已知知识基础上，模糊集对不确定问题的处理往往会得到很好的结果。

粗糙集理论是 1982 年被提出来的。经典的粗糙集模型建立在等价关系的基础上，引入上、下近似的概念，建立了粗糙集理论和方法，其关键在于等价关系。由于粗糙集理论和方法不需要任何先验知识，因此在实际中得到了快速的发展和应用。

随着科学技术的迅猛发展，复杂系统、不确定信息处理日益成为人们生产、生活、社会、经济等活动中出现的新需求；模糊集和粗糙集在处理这些不确定信息时固然有它的优势，而在实际问题中，如果单一地依赖于某一种方法，其结果往往并不理想。所以，模糊集和粗糙

集包括它们的扩展模型的结合，以及它们与其他方法（如人工神经网络）的结合研究，已经成为一个新的研究和应用热点。

参 考 文 献

[1] 施恩伟．模糊集合论基础．成都：西南交大出版社，1994．
[2] 肖盛燮．模糊数学与工程应用．成都：成都科大出版社，1993．
[3] 谢季坚，刘承平．模糊数学方法及其应用（第二版）．武汉：华中科大出版社，2000．
[4] 王士同．模糊系统、模糊神经网络及应用程序设计．上海：上海科学技术文献出版社，1998．
[5] 邹进．模糊集理论在水资源系统分析中的应用研究．华中科技大学博士学位论文，2003．
[6] Pawlak Z．Rough sets：theoretical aspects of reasoning about data．Kluwer Academic Publishers, Boston, 1991．
[7] 年福忠．粗糙集及其在 KDD 中的应用研究．兰州理工大学硕士学位论文，2004．
[8] 赵曦滨，井然哲，顾明基．基于粗糙集的自适应入侵检测算法．清华大学学报（自然科学版）．2008：1165-1168．
[9] Tzung-Pei Hong, Yan-Liang Liou, Shyue-Liang Wang． Fuzzy rough sets with hierarchical quantitative attributes．Expert Systems with Applications．2009:6790-6799．
[10] 年福忠，李明．一种对ε-indiscernibility 相似关系的改进算法．计算机应用研究．2004：145-146．
[11] 史忠植．知识发现．北京：清华大学出版社，2002．
[12] 张文修，吴伟志，梁吉业，李德玉．粗糙集理论与方法．北京：科学出版社，2001．

Chapter 3

第3章 人工神经网络

3.1 人工神经网络概述

人工神经网络[1]（Artificial Neural Network, ANN）是在现代神经科学研究成果的基础上提出来的，主要关注人脑的微观结构，力图从人脑的物理结构上去研究人的智慧产生和形成过程。它是由大量类似于神经元的简单处理单元广泛相互连接而成的复杂网络系统，反映了人脑功能的若干作用，但并非神经系统的真实描写，而只是对其的简化、抽象和模拟。ANN以生物神经网络为模拟基础，以非线性大规模并行处理为主要特征，在诸如模式识别、聚类分析及计算机视觉等方面发挥着许多不可替代的作用。

神经网络模型的基本模式是由大量简单的计算单元（又称为节点或神经元）广泛相互连接而构成的一种并行分布处理网络。基于神经信息传输的原理，各个节点通过可变的权值彼此相连接，每个节点对 N 个加权的输入求和，当和超过某个阈值时，节点呈“兴奋”状态，有信号输出。节点的特征由其值、非线性函数的类型所决定，而整个神经网络则由网络拓扑、节点特征，以及对其进行训练所使用的规则所决定。权值反映了节点之间传递信息时互连的相对强度，对神经网络的功能是至关重要的。

ANN通过权值的调整，表现出类似人脑的学习、归纳和分类，它通过有自学习、自组织和自适应功能的神经网络上的非线性动力学，对无法语言化的模式信息进行处理。它能通过学习功能来实现自适应，自动获得用数据（精确的或模糊的）表达的知识，在自适应及自学习方面已显示出了不少新的前景和新的思路。ANN可通过示例学习，形成描述复杂非线性系

统的非线性函数，这实际上是得到了客观规律的定性描述。有了这个基础，再加上 ANN 模型力图模仿生物神经系统，通过接受外部输入的刺激，不断获得并积累知识，进而具有一定的判断能力，预测的难题就会迎刃而解。

3.1.1 神经元理论[2]

人工神经网络是通过模拟生物神经系统的结构和功能来进行智力活动的。生物神经系统的基本单元是生物神经元。它由细胞体、一个轴突和若干个树突组成。细胞体是接收和处理信息的部件，轴突是向外输出信息的部分，其末端分裂为许多分支。树突相当于神经元的输入，分支很多，用来接受来自其他神经元轴突送来的信息。神经元之间的连接为突触，它是其中一个神经元的轴突的末端。一个神经元到其他神经元的信息传递是经由轴突的末端——突触到另外一个神经元的树突而实现的。当多个树突的输入信息经复合后足够强时，就会激发此神经元产生一个输出信号。

神经元是生物神经系统的最基本单元，虽然其形状大小是多样的，但从功能结构角度而言，各个神经元是相似的。人工神经元模型是生物神经元的数学抽象与模拟，它从功能特性角度对生物神经元进行模拟，形成人工神经网络的基本组成单位。人工神经元通常为多输入、单输出的非线性单元，其数学模型如图 3.1 所示。

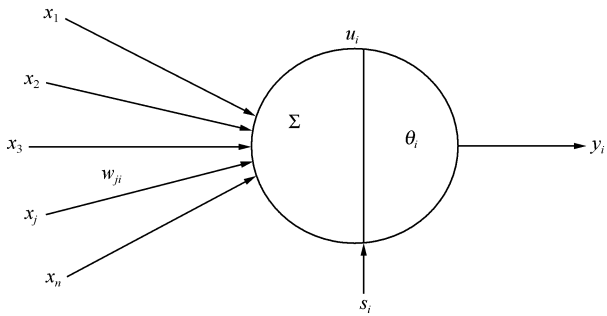


图 3.1 人工神经元数学模型

神经元模型[3]有三个基本要素：

（1）一组连接（对应于生物神经元的突触）。连接强度由各连接上的权值表示，权值为正表示激活，为负表示抑制。

（2）一个求和单元。用于求取各输入信号的加权和（线性组合）。

（3）一个非线性激活函数。起到非线性映射作用并将神经元输出幅值限制在一定范围内（一般限制在（0, 1）或（−1, 1）之间）。

其中，u_i 为神经元 i 的内部状态，θ_i 为阈值，x_j 为输入信号，w_{ji} 表示神经元 j 到神经元 i 的连接权值，s_i 表示外部输入的控制信号，y_i 为神经元 i 的输出值。神经元模型常用一阶微分方程来描述（模拟生物神经网络突触膜电位随时间变化的规律），即：

$$\tau \frac{\mathrm{d}u_i}{\mathrm{d}t} = -u_i + \sum w_{ji} x_j(t) - \theta_i \tag{3.1}$$

$$y_i(t) = f[u_i(t)] \tag{3.2}$$

神经元的输入函数常用函数 f 来表示，通常情况下我们常用以下函数来表达其非线性特性。

（1）阈值函数：该函数为阶跃函数。

$$f(u_i) = \begin{cases} 1, & u_i \geqslant 0 \\ 0, & u_i < 0 \end{cases}$$

（2）分段线性函数：

$$f(u_i) = \begin{cases} 1 & u_i \geqslant u_2 \\ au_i + b, & u_1 < u_i < u_2 \\ 0, & u_i \leqslant u_1 \end{cases}$$

（3）S 型函数：

$$f(u_i) = \frac{1}{1 + \exp(-u_i / c)^2}$$，其中 c 为常数

S 型函数反映了神经元的饱和特性，由于其函数连续可导，调节曲线的参数可以得到类似阈值函数的功能，因而被广泛用做神经元输出函数。

3.1.2　神经网络的拓扑结构[4]

根据神经元之间连接类型的不同，可将人工神经网络分为两大类：分层型神经网络和相互连接型神经网络。

分层型神经网络将一个网络模型中的所有神经元功能分为若干层，一般有输入层、中间层和输出层，各层顺序连接。输入层接收外部的输入信号，并由各输入单元传送给直接相连的中间各单元。中间层是神经网络的内部处理单元层，与外部无直接连接。神经元网络所具有的模式变换能力，如模式分类、模式完善、特征抽取等，主要是由中间层进行的。根据处理功能的不同，中间层可以有多层，也可以没有。由于中间层单元不直接与外部输入/输出打交道，故常将中间层称为隐含层。输出层是网络输出运行结果并与显示设备或执行机构相连

接的部分，如图 3.2 所示。分层型神经网络可以细分为三种互连形式：简单的前向网络、具有反馈的前向网络，以及层内有相互连接的前向网络。

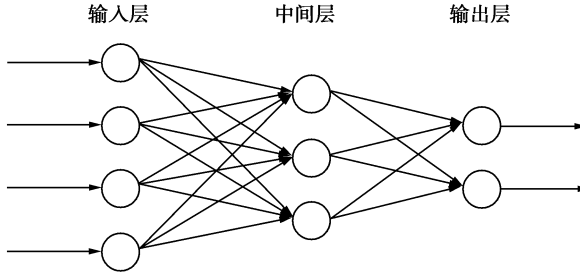


图 3.2　分层型神经网络

相互连接型神经网络是指网络中的任意两个单元都是可以相互连接的，如 Hopfield 网络、波尔茨曼网络均属此类型，如图 3.3 所示。

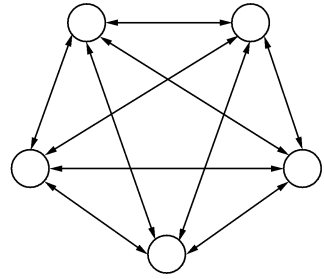


图 3.3　相互连接型神经网络

3.1.3　人工神经网络的学习和训练

神经网络的学习也称为训练，指的是通过神经网络所在环境的刺激作用调整神经网络的自由参数，使神经网络以一种新的方式对外部环境做出反应的一个过程。学习规则是指针对学习问题的明确规则集合，不同的学习规则对神经元的突触权值调整的表达式有所不同。人工神经网络的学习规则很多，但主要可分为两大类：有导师学习规则和无导师学习规则。

（1）有导师学习规则。有导师学习又称为有监督学习（Supervised Learning），在学习时需要给出导师信号或称为期望输出（响应）。神经网络对外部环境是未知的，但可以将导师看做对外部环境的了解，由输入/输出样本集合来表示。导师信号或期望响应代表了神经网络执行情况的最佳结果，即对于网络输入调整网络参数，使得网络输出逼近导师信号或期望响应。

（2）无导师学习规则。无导师学习包括强化学习（Reinforcement Learning）与无监督学习（Unsupervised Learning）或称为自组织学习（Self-Organized Learning）。在强化学习中，对输入/输出映射的学习是通过与外界环境的连续作用最小化性能的标量索引而完成的。在无监督学习中没有外部导师或评价来统观学习过程，而是提供一个关于网络学习表示方法质量的测量尺度，根据该尺度将网络的自由参数最优化。一旦网络与输入数据的统计规律性达成一致，就能够形成内部表示方法作为输入特征编码，并由此自动得出新的类别。通常采用的学习规则有：Herb 学习规则、纠错学习规则、记忆学习规则、随机学习规则和竞争学习规则等。

按运行方式，人工神经网络可划分为前馈式网络和反馈式网络。

（1）前馈式网络。它利用连接强度及神经元的非线性输入/输出关系，实现从输入状态空间到输出状态空间的非线性映射。前馈神经网络在人工神经网络发展史上产生过重大影响，并且是目前最为流行的神经网络模型之一。前馈网络广泛地用于模式分类、特征抽取等方面。

（2）反馈式网络。所有神经元都是计算单元，同时可接受输入，并向外界输出。

3.2　BP 神经网络

BP（Back Propagation）神经网络[5]是 D.E.Rumelhart 和 J.L.McCell 及其研究小组在 1986 年研究并设计出来的，其网络结构简单，算法成熟，且具有精确寻优等优点，在许多应用领域已取得很好的成果。BP 网络主要应用于以下几方面。

（1）函数逼近：用输入矢量和相应的输出矢量训练网络去逼近一个函数。

（2）模式识别：用一个特定的输出矢量将它与输入矢量联系起来。

（3）分类：把输入矢量以所定义的方式进行分类。

（4）数据压缩：减少输出矢量维数以便于传输或存储。

3.2.1　BP 人工神经网络结构

由误差反向传播算法（BP 算法）训练的多层前馈人工神经网络，也称为 BP 人工神经网络，是人工神经网络分类器中最普遍、最通用的形式。已经证明：由一个单隐含层和非线性兴奋函数组成的多层前馈人工神经网络，是通用的分类器。也就是说，这样的网络能逼近任意复杂的决策边界。图 3.4 给出一个多层前馈人工神经网络的拓扑结构示例。这种神经网络模型的特点是：各层神经元之间无反馈连接；各层内神经元之间无任何连接；仅相邻层神经元之间有连接。在图 3.4 中的前馈神经网络中，输入与输出关系是一个高度非线性映射关系，如果输入节点数是 n，输出节点数是 m，则网络是从 n 维欧氏空间到 m 维欧氏空间的映射。实

际计算过程中，往往将代表待识别模式的输入矢量输入至输入层，向前传播到隐节点，经过作用函数之后，通过连接权输出到输出层，最后给出输出结果。该网络中每个神经元通过求输入权值和非线性兴奋函数传递结果来工作，其数学描述如下：

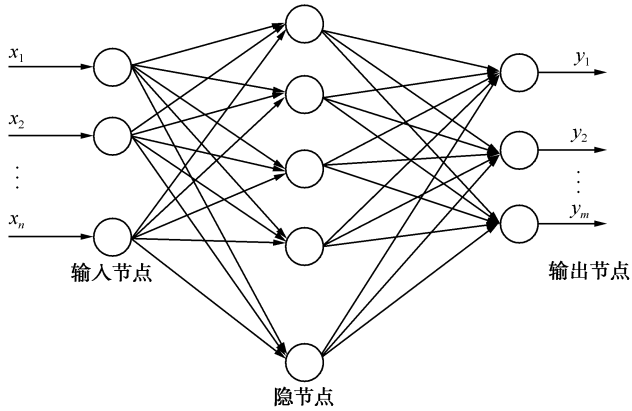


图 3.4　一个多层前馈人工神经网络的拓扑结构示例

$$\text{out}_i = f(\text{net}_j) = f(\sum_{j=1}^{n} w_{ji}x_j - \theta_i), j \neq i \tag{3.3}$$

这里 out_i 是所考虑层中第 i 个神经元的输出；net_j 是前一层第 j 个神经元的输出；w_{ji} 为隐含层神经元 i 与输入层神经元 j 的连接权值；θ_i 为隐含层神经元的阈值。选择一定的函数作为隐含层神经元的激发函数 $f(x)$，如采用 Sigmoid 函数：

$$f(\text{net}_i) = \frac{1}{1+\text{e}^{-\text{net}_i}} \tag{3.4}$$

输出层神经元的输出公式类似隐含层神经元的输出公式。

人工神经网络应用于模式识别问题包括两个截然不同的阶段。第一阶段，即网络训练阶段，如图 3.5 所示调整网络权值以表现问题域（其中 $x_1, x_2, \cdots, x_n$ 为训练数据）。第二阶段，即网络工作阶段，权值固定不变，当把实验数据或实际数据（即图 3.6 中的 $x_1, x_2, \cdots, x_n$，通常称为测试数据）输入到网络时，网络能够对其分类。

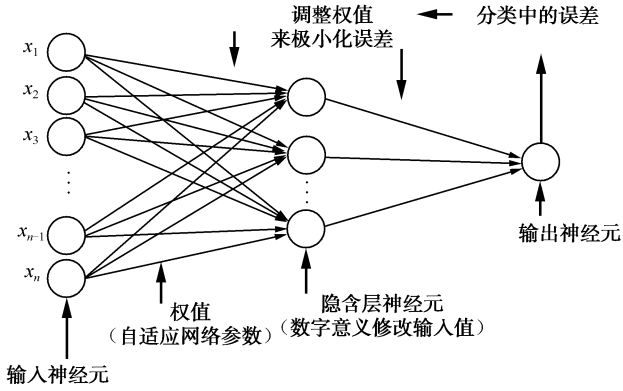


图 3.5　网络训练阶段

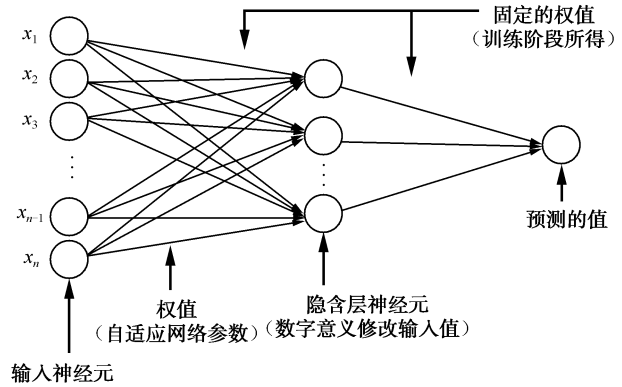


图 3.6　网络工作阶段

网络训练过程，包括从训练集合到权值集合的映射。至少在给定误差内，该组权值可对训练集矢量正确分类。实际上，网络所学正是训练集合所教。如果合理选择训练集合，并且训练算法有效，那么网络应能正确对不属于训练集合的输入量分类。具有自学习能力是神经网络的最重要特征之一，也是利用它来解决实际问题的最重要依据之一。BP 神经网络通过对样本进行学习，调整 BP 神经网络中的连接权值、网络的规模（包括 n，m 和隐含层节点数），就可以实现非线性分类等问题，进而达到非逻辑归纳。因此，BP 神经网络学习算法具有示例学习的特征，利用它可以实现多层前馈神经网络的权值调节。

3.2.2 BP 算法的基本思想[6]

BP 人工神经网络的学习算法称为误差反向传播算法或 BP 学习算法。误差反向传播算法本质上是工程上常用的最小均方算法的一种广义形式，BP 算法使用梯度搜索技术，按代价函数最小的准则递归地求解网络的权值和各节点的阈值，代价函数为网络的实际输出和期待输出的均方误差。网络训练开始时，权值和节点阈值初始化为一组随机值，节点输出的期望值是预先规定的，当输入训练数据后，网络的代价函数可以计算出来，通过 BP 算法，误差逐层向输入层方向逆向传播，使网络不断自适应地修改网络权值和节点阈值，以减小代价函数值，直到它减小到一个可接受的阈值或者不再减小为止。

如图 3.4 所示的 BP 多层前馈人工神经网络的拓扑结构，网络不仅有输入层节点、输出层节点，而且有一层或多层隐含层节点。对于输入信息，要先向前传播到隐含层的节点上，经过各单元的 Sigmoid 型激活函数（又称作用函数、转换函数或映射函数等）运算后，把隐含层节点的输出信息传播到输出节点，最后给出输出结果。

网络的学习过程由正向和反向传播两部分组成：在正向传播过程中，每一层神经元的状态只影响下一层神经元网络，如果输出层不能得到期望输出，也就是说实际输出值与期望输出值之间有误差，那么转入反向传播过程。反向传播过程将误差信号沿原来的连接通路返回，通过修改各层神经元的权值，逐次地向输入层传播去进行计算，再经过正向传播过程。这两个过程反复地进行，使得误差信号最小。实际上，误差达到人们所希望的要求时，网络的学习过程就结束了。

3.2.3 BP 网络学习算法

BP 算法需要导师的指导，是适合于多层神经元网络的一种学习算法，建立在梯度下降法的基础上。

设有 N 个学习样本 $(\boldsymbol{x}_k, \boldsymbol{y}_k)(k=1,2,\cdots,N)$，其中 $\boldsymbol{x}_k$ 为输入向量，$\boldsymbol{y}_k$ 为期望输出向量。设 $I_{jk}^{(l)}$ 表示样本 k 的输入向量 $\boldsymbol{x}_k$ 输入后，传播到第 l 层节点 j 的输入。$O_{jk}^{(l)}$ 表示第 l 层节点 j 的输出，$w_{ij}^{(l)}$ 为第 $l-1$ 层的节点 i 连接第 l 层节点 j 的权值，$n^{(l-1)}$ 为第 $l-1$ 层的节点数，f 为节点神经元的激活函数，BP 人工神经网络的神经元激活函数一般使用可微的 Sigmoid 型函数。由 BP 人工神经网络神经元的输入/输出关系，有：

$$I_{jk}^{(l)} = \sum_{i=1}^{n^{(l-1)}} w_{jk}^{(i)} O_{ik}^{(l-i)} \tag{3.5}$$

$$O_{jk}^{(l)} = f(I_{jk}^{(l)}) \tag{3.6}$$

$f(\bullet)$ 为 Sigmoid 型函数，样本 k 对节点 j 的期望输出 $O_{jk}^{*(l)}$ 与样本 k 对节点 j 的实际计算输出 $O_{jk}^{(l)}$ 的误差定义为：

$$E_{jk}^{(l)} = \frac{1}{2}(O_{jk}^{*(l)} - O_{jk}^{(l)})^2 \tag{3.7}$$

若第 l 层是 BP 人工神经网络的输出层，即节点 j 是输出节点，则 $O_{jk}^{*(l)} = y_{jk}^{*}$，$O_{jk}^{(l)} = y_{jk}$，样本 k 的输出误差为：

$$E_{jk}^{(l)} = \frac{1}{2}(y_{jk}^{*} - y_{jk})^2 \tag{3.8}$$

若对 N 个学习样本的任一样本 k 有输出层的 m 个输出节点的计算输出都分别满足样本 k 的 m 个期望输出，即有 $E_{jk}^{(l)} \leqslant \varepsilon, j = 1,2,\cdots,m$，则学习过程结束。$\varepsilon$ 为指定的允许误差；否则，由误差反向传播过程修改权值分布 w。

按误差的负梯度来修改权值，即：

$$w_{ij}^{(l)} = w_{ij}^{(l)} + \Delta w_{ij}^{(l)} \tag{3.9}$$

$$\Delta w_{ij}^{(l)} = -\eta \frac{\partial E_{jk}^{(l)}}{\partial w_{ij}^{(l)}} \tag{3.10}$$

其中，η 为学习率，$0<\eta<1$。

由式（3.5），式（3.6）可知：

$$\frac{\partial E_{jk}^{(l)}}{\partial w_{ij}^{(l)}} = \frac{\partial E_{jk}^{(l)}}{\partial O_{jk}^{(l)}} \frac{\partial O_{jk}^{(l)}}{\partial I_{jk}^{(l)}} \frac{\partial I_{jk}^{(l)}}{\partial w_{ij}^{(l)}} = \delta_{jk}^{(l)} \frac{\partial I_{jk}^{(l)}}{\partial w_{ij}^{(l)}} = \delta_{jk}^{(l)} O_{ik}^{(l-1)} \tag{3.11}$$

其中，

$$\delta_{jk}^{(l)} = \frac{\partial E_{jk}^{(l)}}{\partial O_{jk}^{(l)}} \frac{\partial O_{jk}^{(l)}}{\partial I_{jk}^{(l)}} = \frac{\partial E_{jk}^{(l)}}{\partial O_{jk}^{(l)}} f'(I_{jk}^{(l)}) \tag{3.12}$$

为了求得 $\delta_{jk}^{(l)}$ 的表达式，进行下述讨论。

（1）若第l层是输出层，则由式（3.8）有：

$$\frac{\partial E_{jk}^{(l)}}{\partial O_{jk}^{(l)}}=\frac{\partial E_{jk}^{(l)}}{\partial y_{jk}}=-(y_{jk}^{*}-y_{jk}) \tag{3.13}$$

由式（3.12），式（3.13）有：

$$\delta_{jk}^{(l)}=-(y_{jk}^{*}-y_{jk})f'(I_{jk}^{(l)}) \tag{3.14}$$

由式（3.10），式（3.11），式（3.14）有：

$$\Delta w_{ij}^{(l-1)}=-\eta\delta_{jk}^{(l)}O_{ik}^{(l-1)}=\eta(y_{jk}^{*}-y_{jk})f'(I_{jk}^{(l)})O_{ik}^{(l-1)} \tag{3.15}$$

（2）若第l层不是输出层，对于隐含层中的目的神经元j，不能直接对误差函数求微分，需要利用微分公式：

$$\frac{\partial E_{jk}^{(l)}}{\partial O_{jk}^{(l)}}=\sum_{q=1}^{n^{(l+1)}}\frac{\partial E_{qk}^{(l+1)}}{\partial I_{qk}^{(l+1)}}\frac{\partial I_{qk}^{(l+1)}}{\partial O_{jk}^{(l)}} \tag{3.16}$$

对第$l+1$层的节点q，类似第l层的节点有：

$$I_{qk}^{(l+1)}=\sum_{j=1}^{n^{(l)}}w_{jq}^{(l)}O_{jk}^{(l)} \tag{3.17}$$

$$O_{qk}^{(l+1)}=f(I_{qk}^{(l+1)}) \tag{3.18}$$

$$E_{qk}^{(l+1)}=\frac{1}{2}(O_{qk}^{*(l+1)}-O_{qk}^{(l+1)})^2 \tag{3.19}$$

$$\delta_{qk}^{(l+1)}=\frac{\partial E_{qk}^{(l+1)}}{\partial I_{qk}^{(l+1)}} \tag{3.20}$$

因此，可把式（3.16）表示为：

$$\frac{\partial E_{jk}^{(l)}}{\partial O_{jk}^{(l)}}=\sum_{q=1}^{n^{(l+1)}}\frac{\partial E_{qk}^{(l+1)}}{\partial I_{qk}^{(l+1)}}\frac{\partial I_{qk}^{(l+1)}}{\partial O_{jk}^{(l)}}=\sum_{q=1}^{n^{(l+1)}}\delta_{qk}^{(l+1)}w_{jq}^{(l+1)} \tag{3.21}$$

由式（3.12），式（3.21）得：

$$\delta_{jk}^{(l)} = f'(I_{jk}^{(l)}) \sum_{q=1}^{n^{(l+1)}} \delta_{qk}^{(l+1)} w_{jq}^{(l+1)} \tag{3.22}$$

由式（3.10），式（3.11），式（3.22）有：

$$\Delta w_{ij}^{(l)} = -\eta \delta_{jk}^{(l)} O_{ik}^{(l-1)} = -\eta f'(I_{jk}^{(l)}) \sum_{q=1}^{n^{(l+1)}} \delta_{qk}^{(l+1)} w_{jq}^{(l+1)} O_{ik}^{(l-1)} \tag{3.23}$$

式（3.14）和式（3.21）给出误差反向传播时输出层各节点和隐含层各节点的权值的关系，由式（3.14）计算出输出层的各节点的 δ 值后，就可由式（3.22）反向逐层计算出各隐含层的所有节点的 δ 值。由各节点的 δ 值，采用式（3.15）或式（3.23），就可计算出各节点的权值修改量 Δw，从而对权值进行修改。

3.3　RBF 神经网络

1985 年 Powell 提出了多变量插值的径向基函数（Radial Basis Function,RBF）方法[7]。1988 年，Broomhead 和 Lowe 首先将 RBF 应用于神经网络设计，对径向基函数和多层神经网络进行了对比，揭示了两者的关系。Moody 和 Darke 在 1989 年提出了一种新颖的神经网络——径向基函数神经网络（Radial Basis Function Neural Network, RBFNN）。同年，Jackon 论证了径向基函数网络对非线性连续函数的一致逼近性能。RBF 神经网络这一新颖的网络类型的出现，给神经网络的研究及应用带来了新的生机。RBF 神经网络可以根据问题确定相应的网络拓扑结构，学习速度快，不存在局部最小问题。它的优良特性使得它在越来越多的领域内成为替代 BP 网络的一种新型网络。

径向基函数（RBF）是一种将输入矢量扩展或预处理到高维空间的神经网络学习方法，其结构十分类似于多层感知器（MLP）。RBF 网络的理论基础是函数逼近，它用一个二层的前向网络去逼近任意函数。网络输入的数目等效于所研究问题的独立变量数目。中间层与输入完全连接（权值=1），中间层节点选取径向基函数作为转移函数，其中包含一个称为中心的参数向量；节点计算输入向量与中心的欧氏距离，然后通过转移函数进行变换。输出层的节点是一线性组合器。

3.3.1　RBF 神经网络结构[8]

RBF 神经网络属于多层前向网络。同许多 BP 网络一样，它也是一种三层静态前向网络，

其拓扑结构如图 3.7 所示。第一层为输入层，由信号源节点组成；第二层为隐含层，其神经元数目视所描述问题的需要而定；第三层为输出层，它对输入模式的作用做出响应。

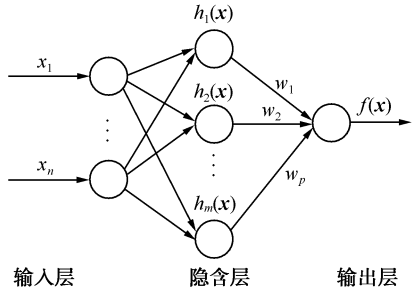


图 3.7　RBF 神经网络拓扑结构

构成 RBF 神经网络的基本思想是：用径向基函数作为隐含层神经元单元的“基”构成隐含层空间，这样就将输入矢量直接（而不通过权值连接）映射到隐含层空间，当径向基函数的中心点确定以后，这种映射关系也就确定了，并且这种映射关系是非线性的，而隐含层空间到输出层空间的映射是线性的，即网络的输出是隐含层神经元单元输出的线性加权和。

3.3.2　RBF 神经网络的映射关系

由上面的分析可知，RBF 神经网络的映射关系由两部分组成（设输入维数为 n，隐单元数为 m，输出维数为 p）。

第一部分：从输入空间到隐含层空间的非线性变换层。

$$h_j(\boldsymbol{x}) = \phi(\|\boldsymbol{x} - \boldsymbol{c}_j\|, \sigma_j) = \exp\left(-\frac{\|\boldsymbol{x} - \boldsymbol{c}_j\|^2}{2\sigma_j^2}\right) \tag{3.24}$$

其中，$\phi(\bullet)$ 为隐含层单元的变换函数（即径向基函数），它是一种局部分布的、对中心点径向对称衰减的非负非线性函数，一般取高斯函数；$\|\bullet\|$ 表示范数，通常取二阶范数；$\boldsymbol{x}$ 为 n 维输入向量，即 $\boldsymbol{x} = \{x_1, x_2, \cdots, x_n\}$；$\boldsymbol{c}_j$ 为第 j 个隐含层单元的中心；σ_j 为第 j 个隐含层单元非线性变换函数的宽度。

第二部分：从隐含层空间到输出层空间的线性合并层。

$$f(\boldsymbol{x})=\sum_{j=1}^{m}h_j(\boldsymbol{x})w_j \tag{3.25}$$

其中，w_j 为第 j 个隐含层单元与输出之间的连接权；m 为隐单元数。

在 RBF 网络中，隐含层执行的是一种固定不变的非线性变换，将输入空间映射到一个新的空间，输出层在该新的空间中实现线性组合器的功能，可调节的参数就是该线性组合器的权值。构造和训练一个 RBF 神经网络就是要使映射函数通过学习，确定出每个隐含层神经元基函数的中心 $\boldsymbol{c}_j$、宽度 σ_j，以及隐含层到输出层的权值 w_j 这些参数，从而可以完成所需的从输入到输出的映射。与 BP 网络单纯由权参数构成不同，RBF 网络的三部分参数在映射中所起的作用是不同的。隐含层的中心和宽度代表了样本空间模式及各中心的相对位置，完成的是从输入空间到隐含层空间的非线性映射，而输出层的权值实现的是从隐含层空间到输出空间的线性映射。必须明确，RBF 网络的核心是隐含层的设计，中心和宽度的选取合适与否将从根本上影响 RBF 网络的最终性能[9,10]。

在 RBF 网络结构中，对于训练样本 $\left\{(x_i,\hat{y}_i)\right\}_{i=1}^{p}$，通常取性能指标为：

$$E=\sum_{i=1}^{p}(\hat{y}_i-f(x_i))^2 \tag{3.26}$$

如果在误差准则的基础上加上一项惩罚项，则性能指标可以写为：

$$E=\sum_{i=1}^{p}\left(\hat{y}_i-f(x_i)^2\right)+\sum_{j=1}^{m}\lambda_j w_j^2 \tag{3.27}$$

其中，λ 为惩罚因子，通过引入惩罚项来迫使参数的调整产生平滑的逼近（规范化方法）。

根据 RBF 神经网络映射关系，其数学描述可以写为：

$$\begin{aligned}f(\boldsymbol{x})&=\sum_{j=1}^{m}h_j(\boldsymbol{x})w_j\\&=\sum_{j=1}^{m}\exp\left(-\frac{\left\|\boldsymbol{x}-\boldsymbol{c}_j\right\|^2}{2\sigma_j^2}\right)w_j\end{aligned} \tag{3.28}$$

通过上述描述可知，指标 E 是关于中心 $\boldsymbol{c}$、宽度 σ 和权值 w 的函数。RBF 网络的训练就是针对一组样本，使 E 趋于最小。从而我们可以发现，RBF 网络中所利用的非线性径向基函数的形式对网络性能的影响并不是至关重要的，关键因素是对径向基函数中心、宽度和权值的确定。对于输出层的权重可以通过 delta 规则或一些其他传统的统计方法，如伪逆矩阵来确定。对于大样本输入，如果每个训练样本都用来作为径向基函数的中心，那么网络将变得非

常庞大，难以处理，而且会倾向于过拟合；如果从训练样本中随机选取一个子集作为网络的中心，就不能满足带噪声的样本。常用的方法是首先对样本进行聚类，以聚类中心作为隐含层神经元的中心，这个过程通常是无导师学习过程；然后以每个样本为学习样本对神经网络进行训练以对输出权值进行修改，这个过程称为有导师的学习过程。

3.3.3 RBF 网络学习算法[11]

确定 RBF 神经网络结构最主要的是确定基函数中心，基函数的宽度和输出层的权值。当前的 RBF 学习算法基本可以分为两类，一类是两阶段学习法，即通过聚类等方法确定基函数的中心和宽度，该阶段为无导师学习，然后通过有导师的训练确定输出层的权值。另外一类是 RBF 网络的动态全监督学习算法，即在神经网络学习之前不确定神经网络的结构，而在神经网络的学习过程中逐渐地增大或缩小网络的结构，直到满意为止。

1．基于聚类的 RBF 神经网络学习算法

该算法属于传统的 RBF 神经网络学习算法[12]，往往通过聚类的方法确定隐含层函数的中心和宽度。在这一阶段常用的算法有 K-Means 聚类算法、基于密度的聚类算法等。基于密度的聚类算法的基本思想是在样本空间中，每一个样本点都受其他样本点的影响，任意两点间的影响程度可以由下式来表示：

$$P_i = \mathrm{e}^{-\alpha\left\|\boldsymbol{x}_i-\boldsymbol{x}_j\right\|^2} \tag{3.29}$$

其中，P_i 为 $\boldsymbol{x}_j$ 对 $\boldsymbol{x}_i$ 的影响：$\alpha = 4/R_\alpha^2$。R_α 是一个常数，表示邻域半径。如果 $\boldsymbol{x}_j$ 在 $\boldsymbol{x}_i$ 的邻域半径 R_α 内，则 P_i 会很大，否则 P_i 会很小。

因此，该样本点处的密度可以表示为：

$$T_i = \sum_{j=1}^{n} \mathrm{e}^{-\alpha\left\|\boldsymbol{x}_i-\boldsymbol{x}_j\right\|^2}\ ，\text{其中 } j \neq i \tag{3.30}$$

点 $\boldsymbol{x}_i$ 周围聚集的样本点越多，$\boldsymbol{x}_i$ 处的密度也就越大。基于密度聚类的 RBF 神经网络学习算法步骤如下。

Step 1：初始化，确定邻域半径 R_α 和密度阈值 t。

Step 2：计算每一个点处的密度 T_i，$i = 0,1,\cdots,n$。

Step 3：如果存在 $T_i > t$，则将所有大于 t 的密度值排序，然后转 Step 4，如果所有的密度值都小于 t，则转 Step 6。

Step 4：选择密度最大的点 $\boldsymbol{x}_p$，作为聚类中心点。

Step 5：在所有剩余的样本点 $\boldsymbol{x}_s$ 的密度值中，减去点 $\boldsymbol{x}_p$ 对 $\boldsymbol{x}_s$ 的密度影响，然后执行 Step 3。

Step 6：对剩下的未被确定为聚类中心的样本点，则按照最短距离法进行聚类，直到所有的点都被聚类为止。

Step 7：以聚类中心作为基函数的中心，以聚类的隶属度作为基函数的宽度构建 RBF 神经网络隐含层单元。

Step 8：对神经网络进行有监督训练，采用 LMS 算法确定输出层权值。

Step 9：神经网络预测。

2．动态全监督 RBF 神经网络学习算法[13, 14]

RBF 网络中用径向基函数作为隐含层神经元的“基”，构成隐空间。这样，在基函数的中心及宽度参数确定后，隐含层执行的是一种固定不变的非线性变换。而每个基函数对于全部输入矢量 $\boldsymbol{x}_p$, p=1,2,⋯, s 的非线性变换作用可由矢量 $\boldsymbol{R}_i=\{\boldsymbol{R}_i(\boldsymbol{x}_1),\boldsymbol{R}_i(\boldsymbol{x}_2)\cdots,\boldsymbol{R}_i(\boldsymbol{x}_n)\}$ $(i=1,2,\cdots,N_h)$ 反映出来。因而我们可以通过比较 $\boldsymbol{R}_i$ 与 $\boldsymbol{R}_j$ $(j=1,2,\cdots,N_h,i\neq j)$，来判断第 i 个隐含层神经元与第 j 个隐含层神经元对输入矢量的非线性变换作用的相似性。若两者的作用相似，则可以删除其中一个或将两个合并为一个，以达到精简隐含层神经元的目的。

判断隐含层神经元对输入矢量的非线性变换作用是否相似时，可将 N_h 个矢量 $\boldsymbol{R}_i(i=1,2,\cdots,N_h)$ 看成是 $\boldsymbol{R}^s$ 空间里的 N_h 个点。当点间距离近时，两矢量的差异小，因而有：

调整规则 1

$$\mathrm{H1}_{ij}=\sum_{p=1}^{S}\left\|\boldsymbol{R}_i(\boldsymbol{x}_p)-\boldsymbol{R}_j(\boldsymbol{x}_p)\right\|^2 \tag{3.31}$$

$$\mathrm{H1}_{i\cdot j\cdot}=\min\{\mathrm{H1}_{ij}\} \tag{3.32}$$

$$\left\langle\overline{\boldsymbol{R}}_i,\overline{\boldsymbol{R}}_j\right\rangle=\frac{\boldsymbol{R}_i}{\left\|\boldsymbol{R}_i\right\|}\bullet\frac{\boldsymbol{R}_j}{\left\|\boldsymbol{R}_j\right\|}=\cos\theta \tag{3.33}$$

其中，$\langle\bullet,\bullet\rangle$ 为空间 $\boldsymbol{R}^s$ 上的内积范数。$\overline{\boldsymbol{R}}_i=\{\boldsymbol{R}_i(x_p)/\left\|\boldsymbol{R}_i\right\|\},p=1,2,\cdots,s;i=1,2,\cdots,N_h$，$\theta$ 为二矢量间的夹角。显然，$\cos\theta$ 越大，$\boldsymbol{R}_i$ 与 $\boldsymbol{R}_j$ 就越相似。由此我们可得：

调整规则 2

$$\mathrm{H2}_{ij}=\left\langle\overline{\boldsymbol{R}}_i,\overline{\boldsymbol{R}}_j\right\rangle \tag{3.34}$$

$$\mathrm{H2}_{i\cdot j\cdot}=\max\{\mathrm{H2}_{ij}\} \tag{3.35}$$

因此，我们可以按照调整规则 1 或调整规则 2 对隐含层神经元进行调整，对那些最相似的神经元加以合并，以缩小神经网络的规模。可以将两种调整规则结合起来构建动态全监督的 RBF 神经网络学习算法，其算法步骤如下。

Step 1：初始化目标矢量 $\boldsymbol{R}$，其中 $\boldsymbol{R}=\{y_1,y_2,\cdots,y_j,\cdots,y_n\}$，$y_j$ 为第 j 个样本的目标值，确定神经网络学习所要达到的精度 t。

Step 2：以每个学习样本为基函数中心，以随机生成的正小数为基函数宽度生成隐含层神经元。

Step 3：学习样本经每个神经元 i 处理后得到映射结果为 $\boldsymbol{R}_i=\{y_1^i,y_2^i,\cdots,y_j^i,\cdots,y_n^i\}$，其中，$y_j^i$ 为第 j 个样本经过第 i 个神经元映射后得到的输出值。

Step 4：根据调整规则 1、调整规则 2 求每一个 $\boldsymbol{R}_j$ 与 $\boldsymbol{R}$ 的矢量内积，并将所得的结果从大到小排序，同时将对应的神经元排序。

Step 5：构建 RBF 神经网络，其中隐含层单元的个数为零。

Step 6：按序取一个神经元，加入到已构建 RBF 神经网络的隐含层中，然后对神经网络进行训练。

Step 7：如果神经网络学习能够达到给定的精度，则转入 Step 8，否则继续执行 Step 6。

Step 8：神经网络预测。

3．权重修改算法——LMS 算法[15]

LMS 算法即最小均方误差算法，由 Widrow 和 Hoff 共同提出。由于它的计算量小、易于实现等特点而得到广泛应用。LMS 算法是基于最陡下降的一种算法，即使权矢量沿着性能函数负梯度的方向逼近其最佳值，其迭代算法公式如下：

$$e(n)=d(n)-\boldsymbol{X}^{\mathrm{T}}(n)\boldsymbol{W}(n) \tag{3.36}$$

$$E(n)=\sum_{i=1}^{m}e_i^2(n) \tag{3.37}$$

$$\boldsymbol{W}(n+1)=\boldsymbol{W}(n)+2\mu e(n)\boldsymbol{X}(n) \tag{3.38}$$

其中，$\boldsymbol{X}(n)=[x_1(n),x_2(n),\cdots,x_L(n)]^{\mathrm{T}}$ 为 n 次 RBF 神经网络隐含层神经元的输出矢量，L 为隐含层神经元的个数。$\boldsymbol{W}(n+1)=[w_1(n),w_2(n),\cdots,w_n(n)]$ 为第 n 次 RBF 神经网络学习时输出层的权值向量；$d(n)$ 为期望输出值；μ 为学习步长或学习率；$e(n)$ 为输出值与期望值的误差；$E(n)$ 为总体均方误差。

3.4　概率神经网络[16]

概率神经网络（Probabilistic Neural Network, PNN）是基于概率统计思想和贝叶斯分类规则构成的分类神经网络。贝叶斯分类规则是具有最小“期望风险”的优化决策规则，它可以处理大量样本的分类问题。概率神经网络在功能上与贝叶斯分类器相同，它通过已知样本数据集的概率密度函数来进行贝叶斯分类，将学习到的权数、平滑参数等用于未知数据的判断，从而判断未知数据最有可能属于哪个已知数据集，其分类结果因具有良好的分类，因此被广泛用于说话人识别、模糊分类、交通方式分类等领域。

与 BP 网络进行比较，概率神经网络主要有以下几方面的优点：

（1）快速运算。由于概率神经网络一次完成，不需要学习，因而大约比 BP 神经网络快 5 个数量级。

（2）只要具有足够的训练数据，不管训练矢量与类别之间具有多么复杂的关系，概率神经网络都能保证获得贝叶斯准则下的最优解，而 BP 神经网络却可能在一个局部最优解处中断，无法保证得到一个全局最优的满意解。

（3）概率神经网络允许在训练集中添加或删除数据而不需要重复训练，BP 神经网络对训练集中的任何变动都需要对整个训练过程重复进行。

（4）概率神经网络给出一个指示基于决策的可信度大小的结果，而 BP 神经网络却不能提供这样的可信度指标，若输入与训练过的不一样，它可能产生一个错误的答案。

概率神经网络除了能克服 BP 神经网络的缺陷外，还能保留 BP 网络所具有的学习、归纳和并行计算的特征，它是径向基函数模型的发展。

3.4.1　概率神经网络结构

PNN 是 RBF 网络的一种变体，特别适合于求解模式识别问题，类似于其他 RBF 网络，PNN 存在一个径向基传递函数环节，它是统计方法与前馈神经网络相结合的一种神经网络模型。PNN 的网络结构如图 3.8 所示，图中 $\boldsymbol{I}_{1,1}$ 为连接输入和第 1 层（径向基函数层）的权重矩阵，$\boldsymbol{I}_{1,1}$ 为 $Q\times R$ 维，Q 为输入目标对的数量，即第 1 层神经元数，R 为预定义的模式类别数，即第 2 层神经元数；$\boldsymbol{P}$ 为待检特征向量($R\times1$)；$\boldsymbol{b}_1$ 为径向基函数层（第 1 层）的阈值，属于阈值向量($Q\times1$)；$\boldsymbol{a}_1$ 为第 1 层中径向基传递函数的输出向量；$\boldsymbol{L}_{2,1}$ 是连接第 1 层和第 2 层（竞争层）的权重矩阵；C 为竞争传递函数。

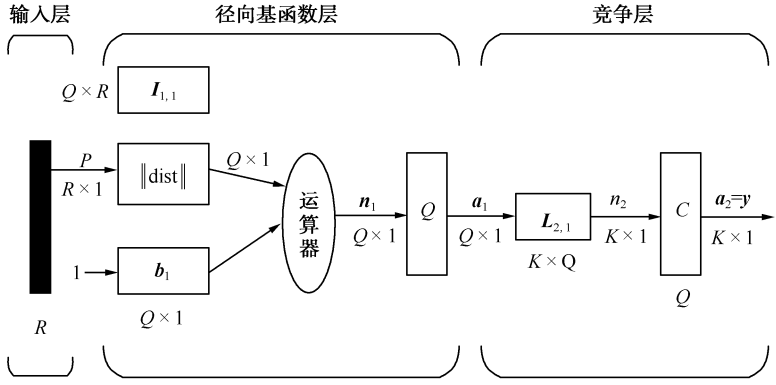


图 3.8 PNN 的网络结构

3.4.2 概率神经网络训练[16, 17]

假设有 Q 组训练向量对 $\boldsymbol{I}_1/\boldsymbol{O}_1, \boldsymbol{I}_2/\boldsymbol{O}_2, \cdots, \boldsymbol{I}_Q/\boldsymbol{O}_Q$，其中 $\boldsymbol{I}$ 为训练向量对中的输入向量($R\times1$)；$\boldsymbol{O}$ 为训练向量对中的目标向量。K 为预定义模式类别数，$\boldsymbol{Q}_i(i=1,2,\cdots,Q)$ 的形式是 K 维向量，K 个分量分别对应 K 个模式类别，其中有且仅有一个分量为 1，其余为 0，表示所对应的输入向量属于与该分量对应的一类模式。训练时，输入以列向量形式组成一个输入矩阵 $\boldsymbol{P}_m$，即训练输入向量矩阵($R\times Q$)，目标向量可组成一个矩阵 $\boldsymbol{T}$，即训练目标向量矩阵($K\times Q$), $\boldsymbol{T}=\left[\boldsymbol{O}_1^{\mathrm{T}},\boldsymbol{O}_2^{\mathrm{T}},\cdots,\boldsymbol{O}_Q^{\mathrm{T}}\right]$。

概率神经网络的训练过程非常简单，网络的 $\boldsymbol{I}_{1,1}$ 被设置为 $\boldsymbol{P}_m$ 的转置矩阵，$\boldsymbol{L}_{2,1}$ 被设置为矩阵 $\boldsymbol{T}$，这样网络训练完成，并且网络的输出矩阵和目标向量矩阵的残差为 0，这是 PNN 最大的优点。

当 $\boldsymbol{P}=\left[p_1,p_2,\cdots,p_n\right]^{\mathrm{T}}$ 输入到已经训练好的网络时，网络的第 1 层计算该输入向量与训练向量集中每一个训练向量的欧氏距离向量：

$$\boldsymbol{D}=\left[d_1,d_2,\cdots,d_Q\right]^{\mathrm{T}} \tag{3.39}$$

$$\boldsymbol{D}=\left[\left\|\boldsymbol{P}-\boldsymbol{I}_1\right\|,\left\|\boldsymbol{P}-\boldsymbol{I}_2\right\|,\ldots,\left\|\boldsymbol{P}-\boldsymbol{I}_Q\right\|\right]^{\mathrm{T}} \tag{3.40}$$

生成向量 $\boldsymbol{D}$ 与 $\boldsymbol{b}_1$ 相乘，相乘的结果用 $\boldsymbol{n}_1$ 表示，即 $\boldsymbol{n}_1$ 为径向基传递函数的输入向量，

$\boldsymbol{n}_1=\left[b_1\left\|\boldsymbol{P}-\boldsymbol{I}_1\right\|,b_1\left\|\boldsymbol{P}-\boldsymbol{I}_2\right\|,\cdots,b_1\left\|\boldsymbol{P}-\boldsymbol{I}_Q\right\|\right]^{\mathrm{T}}$。

$\boldsymbol{n}_1$ 作为径向基函数神经元的输入，得到径向基函数的输出。

$$\boldsymbol{a}_1 = \text{Radbas}(\boldsymbol{n}_1) = \left[a_{1,1}, a_{1,2}, \cdots, a_{1,Q}\right]^{\mathrm{T}} \quad 0 \leqslant a_{1,i} \leqslant 1 \quad i = 1, 2, \cdots, Q \tag{3.41}$$

待检向量与训练向量集中的某个输入向量的欧氏距离越接近，$\boldsymbol{a}_1$ 中相应的位置输出值越接近 1。网络的第 2 层把 $\boldsymbol{a}_1$ 中的分量按模式类别求和，得到概率向量：

$$\boldsymbol{n}_2 = \left[n_{2,1}, n_{2,2}, \cdots, n_{2,k}\right]^{\mathrm{T}} \quad \boldsymbol{n}_2 = \boldsymbol{T} \times \boldsymbol{a}_1 \tag{3.42}$$

$\boldsymbol{n}_2$ 维数为 K，每一个分量对应一个模式类别，分量数值的大小表示待检向量 $\boldsymbol{P}$ 可以归类为该对应模式类别的概率。最后，这个向量还要经过一个竞争传递函数 C ，竞争传递函数的运算规则为：

$$n_{2,i} = \begin{cases} 1 & n_{2,i} = \max(n_{2,1}, n_{2,2}, \cdots, n_{2,K}) \\ 0 & n_{2,i} \neq \max(n_{2,1}, n_{2,2}, \cdots, n_{2,K}) \end{cases} \tag{3.43}$$

运算的目的就是选出概率向量中最大数值的分量，并在竞争层输出向量 $\boldsymbol{a}_2$ 将其置 1，其余元素置 0，表示网络把 $\boldsymbol{P}$ 归类为此模式类别。通过这样一个过程，网络就将待检向量 $\boldsymbol{P}$ 分类到某一类最可能正确的模式，从而完成了模式分类。

对于网络结构的输出节点的选择，决定了多输出型和单输出型两种人工神经网络模型在模式识别中的应用方式。网络结构的输入层的节点数对应于样点数或样本的特征维数，而输出层的节点数等于类别数。在训练阶段，如果用于训练的输入训练样本的类别标号是 i，则训练时设第 i 个节点的期望输出为 1，而其余输出节点期望输出均为 0。在识别阶段，当一个未知类别的样本作用到输入端时，考查各输出节点的输出，并将这个样本的类别判定为输出值最大的那个节点对应的类别。

3.5　小结

人工神经网络是 20 世纪 40 年代末发展起来的一门跨多学科和门类的科学，它在不同程度和层次上模仿人脑神经系统的信息处理功能，从而达到实现人工智能的目的。人工神经网络以非线性大规模并行处理为主要特征，克服了传统人工智能方法对于非结构化信息处理方面的缺陷，具有自适应，自组织和实时学习的特点，在诸如模式识别、系统辨识、信号处理、聚类分析及计算机视觉等方面得到了很好的应用，成功地解决了许多现代计算机难以解决的问题，表现出了良好的智能特性。

人工神经网络正在向模拟人类认知的道路上更加深入地发展，它与模糊系统、遗传算法、进化机制等结合，成为了人工智能的一个重要研究方向，进一步推动了智能信息处理技术的不断进步。

参 考 文 献

[1] 谷萩隆嗣．人工神经网络与模糊信号处理．北京科学出版社，2003．
[2] 李振海，盖潇筱，曾东升．一种结合神经元网络的 PMV 模糊算法．同济大学学报，2008，5(19)：161-167．
[3] 蔺想红，张田文．分段线性脉冲神经元模型的动力学特性分析．电子学报，2009，6(22)：202-211．
[4] 何明，冯博琴，马兆丰，傅向华．一种基于粗糙集的粗糙神经网络构造方法．西安交通大学学报，2004，12(8)：43-52．
[5] 江虹，曾立波．优化的 BP 神经网络分类器的设计与实现．计算机工程与应用，2001，37(5)：122-144．
[6] A.F.R Rahman, M.C. Fairhurst．Multiple classifier decision combination strategies for character recognition: A review. International Journal of Document Analysis and Recognition,2003,5(4): 166-194．
[7] Powell M I D. Radial basis function for multivariable interpolation Review. IMA Conf. on Algorithms for the Approximation of Functions and Data, RMCS Shrivanham,1985．
[8] Broomhead, Lowe D. Radial basis functions, multi-variable functional interpolation and adaptive networks. Complex Systems,1988．
[9] J.E. Moody, C.J. Darken. Fast learning in networks of locally tuned processing units. Neural Computation,1989,1(2):281-294．
[10] I. R. H. Jackson. Convergence properties of radial basis function. Constructive Approximation, 1988, 4(1):243-264．
[11] T. Holcomb, M. Morari. Local training of radial basis function networks：Toward solving the hidden unit problem. American Control Conference,1991．
[12] 周俊武，孙传尧，王福利，径向基函数（RBF）网络的研究及实现．矿冶，2001，12(10)：71-75．
[13] 朱明星，张德龙．RBF 网络基函数中心选取算法的研究．安徽大学学报，2000，24(1)：72-78．

[14] 张铃，张跋．多层前馈神经网络的综合和学习算法．软件学报，1997，8(4)：252-258．
[15] 孙毅刚，战强．一种用于径向基函数（RBF）神经网络训练的有效方法．哈尔滨工业大学学报，1997，29(4)：103-106．
[16] 蔡坚．基于人工神经网络的入侵检测系统的研究与实现．贵州大学硕士学位论文，2005．
[17] 王贞．与文本无关的说话人特征提取及识别方法研究．兰州理工大学硕士学位论文，2006．

Chapter 4

第4章 支持向量机

基于数据的机器学习是现代智能技术中一个十分重要的方面，主要研究如何从一些观测数据（样本）出发得出目前尚不能通过原理分析得到的规律，利用这些规律去分析客观对象，对无法观测的数据进行预测。现有机器学习方法共同的理论基础之一就是统计学。传统统计学所研究的是渐进理论，即当样本数目趋向于无穷大时的极限特性,但实际应用中，样本数目却是有限的，当问题处在高维空间时尤为如此，这是包括模式识别和神经网络等在内的现有机器学习理论和方法中的一个根本问题。N.Vapnik 等人早在 20 世纪 60 年代就开始研究有限样本情况下的机器学习问题。直到 90 年代，在统计学习理论的基础上发展出了一种新的模式识别方法——支持向量机[1]。它在解决小样本、非线性和高维模式识别问题中表现出许多特有的优势，并能够推广应用到函数拟合等其他机器学习问题中。作为统计学习理论的一个新方法，它在医疗诊断、人脸检测与识别、说话人识别等领域的应用成为模式识别领域研究的新热点。

4.1 机器学习问题

从 20 世纪 90 年代开始，机器学习[2]作为一种智能学习方法得到了广泛的研究和应用。它主要是从一系列已知的样本集中推断出蕴涵在样本集中的规则，使机器对今后未知的样本有自学习的能力。机器学习主要有两种方法：一种是无监督的学习，另外一种是有监督的学

习。无监督学习是指样本数据中不包含输出值，学习的任务就是理解数据产生的过程。这样的学习包括密度估计、聚类等方法。目的是将具有相似特征的样本归为一类。

样本是由输入/输出对给出的时候就称为有监督学习，有关输入/输出函数关系的样本就称为训练样本。输入/输出对通常反映了从输入映射到输出的一种函数关系，当存在内在函数 $f(x)$ 时，该函数就称为目标函数。由学习算法输出的对目标函数 $f(x)$ 的估计 $f(x,\alpha),\ \alpha\in\Lambda$ 称为学习问题的解，其中函数 $f(x,\alpha)$ 由 α 控制。对于分类问题，函数 $f(x,\alpha)$ 就称为决策函数。图 4.1 给出机器学习的学习过程。

对于有监督学习，学习的目的是根据给定的训练样本求对某系统输入/输出之间依赖关系 $x_i\rightarrow y_i$ 的估计，使它能够对未知输出做出尽可能准确的预测 $x\rightarrow f(x,\alpha)$。给定一个新输入的样本 x 和一个特定的参数 α，系统将给出一个唯一的输出 $f(x,\alpha)$。函数 $f(x,\alpha)$ 及其参数 α 的产生过程就是我们所说的学习训练。

图 4.1　机器学习的学习过程

设 $\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in\Omega_x\subset\mathbf{R}^n$ 为 n 维矢量空间 Ω_x 中的随机矢量，其分量 $x_i(i=1,2,\cdots,n)$ 为对象的第 i 个特征的测量值（包含检测噪声）；随机矢量 $\boldsymbol{x}$ 有确定的概率分布 $p(\boldsymbol{x})$。设对象的模式可按特征划分为 k 类，用正整数 $y\in\{0,1,\cdots,k-1\}$ 表征，即 $y=i$ 表示对象的模式划分属于第 i 类。当特征矢量为 $\boldsymbol{x}$ 时，模式划分属于 y 的条件概率分布密度为 $p(y/\boldsymbol{x})$，此为后验概率。

若要构造一个分类器进行模式识别，首先要定义一个判别函数 $f(x,a)\in\{0,1,\cdots,k-1\}$，$R=\int R(f(\boldsymbol{x})/\boldsymbol{x})p(\boldsymbol{x})\mathrm{d}\boldsymbol{x}$ 表示当测量矢量为 $\boldsymbol{x}$ 时，将对象判定为第 i $(i=0,1,\cdots,k-1)$ 类。定义损失函数为：

$$L(y,f(\boldsymbol{x},\alpha))=1-\delta_{yf}=\begin{cases}0, & y=f(\boldsymbol{x},\alpha)\\ 1, & y\neq f(\boldsymbol{x},\alpha)\end{cases}\tag{4.1}$$

其中，y 是对象实际所属的类别，而 $f(\boldsymbol{x})$ 是分类器根据决策规则将对象划分的类别。

在已知观测矢量 $\boldsymbol{x}$ 的条件下，决策函数 $f(\boldsymbol{x})$ 所导致的损失的条件期望值为：

$$R(f(\boldsymbol{x})/\boldsymbol{x})=\sum_{y=0}^{k-1}L(y,f(\boldsymbol{x}))p(y/\boldsymbol{x})\tag{4.2}$$

式（4.2）表示测试矢量为 $\boldsymbol{x}$ 时的条件风险。决策中所有可能测量值的总风险 R 称为期望风险：

$$R(a)=\int\frac{1}{2}|y-f(\boldsymbol{x},a)|\mathrm{d}P(\boldsymbol{x},y) \tag{4.3}$$

这样，学习问题就成了在概率密度函数 $P(\boldsymbol{x},y)$ 未知，在已知观测样本是 $(x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n)$ 的条件下，求取使期望风险 $R(a)$ 最小的决策函数 $f^*(\boldsymbol{x},a)$。

而在实际应用中，计算期望风险（即真正的风险）$R(a)$ 是非常困难的，甚至是不可能的。因为求整个样本空间 Ω_x 中的 $P(\boldsymbol{x},y)$ 在应用中是不可能的。

在应用中，常常用经验风险去逼近期望风险。经验风险是指在一个有限的测试集上的平均风险。其公式表示如下：

$$R_{\mathrm{emp}}(a)=\frac{1}{2l}\sum_{i=1}^{l}|\,y_i-f(x_i,a)\,| \tag{4.4}$$

用经验风险逼近期望风险，这一原则称为经验风险最小化（Empirical Risk Minimization）原则，简称 ERM 原则[3]。

仔细研究经验风险最小化原则和机器学习问题中的期望风险最小化的要求，可以发现用经验风险去逼近期望风险，只是直观上的想当然的做法，并没有可靠的理论依据。首先，$R_{\mathrm{emp}}(a)$ 和 $R(a)$ 都是 a 的函数，概率论中的大数定理只说明了当样本趋近于无穷多时 $R_{\mathrm{emp}}(a)$ 将在概率意义上趋近于 $R(a)$，并没有保证使 $R_{\mathrm{emp}}(a)$ 最小的 a 与使 $R(a)$最小的 a 是同一个点，同时，我们不能保证当样本数有限时，$R_{\mathrm{emp}}(a)$ 能趋近于 $R\ (a)$。这一研究很好地解释了在机器学习问题中，当训练保证经验风险最小时，但分类器的分类效果却并不尽如人意的现象。在早期神经网络研究中，人们总是把注意力集中在如何使经验风险更小，但很快发现，一味追求训练误差小并不总能达到很好的预测效果。人们将学习机器对未来输出进行正确预测的能力称为推广性。某些情况下，当训练误差过小反而会导致推广能力的下降。这就是几乎所有神经网络研究者都曾遇到的所谓过学习（Over Fitting）问题。从理论上看，模式识别中也存在同样的问题，但因为通常使用的分类器模型都是相对比较简单的，因此过学习问题并不像神经网络中那样突出。之所以出现过学习现象，一是因为学习样本不充分，二是学习算法设计不合理，这两个问题是互相关联的。在神经网络中，如果对于有限的训练样本来说网络的学习能力过强，足以记住每一个训练样本，此时经验风险很快就可以收敛到很小甚至零，但我们却根本无法保证它对未来新的样本能够得到很好的预测。这就是有限样本下学习机器复杂性与推广性之间的矛盾。

在很多情况下，即使我们已知问题中的样本来自某个比较复杂的模型，但由于训练样本有限，用复杂的预测函数对样本进行学习的效果通常也不如用相对简单的预测函数的学习效果，当有噪声存在时就更是如此。

从这些讨论中我们可以得出以下基本结论：在有限样本情况下，

（1）经验风险最小并不一定意味着期望风险最小；

（2）学习机器的复杂性不但与所研究的系统有关，而且要与有限的学习样本相适应。

有限样本情况下的学习精度和推广性之间的矛盾似乎是不可调和的，采用复杂的学习机器容易使学习误差更小，但却往往丧失推广性。因此，人们研究了很多弥补方法，如在训练误差中对学习函数的复杂性进行惩罚，或者通过交叉验证的方法进行模型选择以控制复杂度等，使原来的方法得到了改进。但是，这些方法多带有经验性质，缺乏完善的理论基础。统计学习理论可以从理论上给机器学习领域中的这一系列困扰的问题找到彻底的答案。

4.2　统计学习理论

统计学习理论[4,5]（Statistical Learning Theory，SLT）就是针对 4.1 节中介绍的经验风险和期望风险之间的关系问题提出的。该理论对用经验风险最小化原则解决期望风险最小化问题的前提是什么，当这些前提不成立时经验风险最小化方法的性能如何，以及是否可以找到更合理的原则等基本问题进行了深入的研究。

其主要内容包括 4 个方面：

（1）经验风险最小化准则下统计学习一致性的条件；

（2）在这些条件下关于统计学习方法推广性的界的结论；

（3）在这些条件的基础上建立的小样本归纳推理准则；

（4）这种推理准则实现的方法。

其中，最有指导性的理论结果是推广性的界，与此相关的一个核心概念是 VC 维。

4.2.1　VC 维

神经网络以经验风险最小化原则为基础，仍存在着许多无法解决的问题。例如，局部极小点问题（即无法从理论上确保网络收敛到全局最优点）、过学习问题、欠学习问题、维数灾难、模型选择等问题。VC 理论严格地证明了 ERM 原理合理性的依据：一致收敛性的充分必要条件、快速收敛的充分条件和一致收敛与概率分布无关的充分必要条件，它们是统计学习渐近理论的 3 个最重要的成果。这些成果的详细表述和严格证明可在 Vapnik 的著作[6]中找到。

更重要的是，通过渐近理论的研究导出了一个十分重要的表达函数集复杂性的容量概念——VC 维数，它在更有实际意义的非渐近理论中是一个关键的概念。VC 维数是式（4.3）中的近似函数组 $f(\boldsymbol{x},\alpha),\ \alpha\in\Lambda$ 的一个属性，其定义与函数类型有关。下面以模式识别中划

分为两类的简单问题为例来说明这个概念。此时函数组为 $f(\boldsymbol{x},\alpha)\in\{+1,-1\}(\forall \boldsymbol{x},\alpha)$，这种函数分别用 +1 和 –1 标记两类不同的样本点，称为指示函数。l 个样本划分为两类，共有 2^l 种不同的分法，若对所有这些分法，都能在 $f(\boldsymbol{x},\alpha)$ 中找到一个指示函数给出正确的分类标记，则称函数组 $f(x,\alpha)$ 能将这 l 个样本点分完。一个指示函数组能分完的样本点的最大数目称为该函数组的 VC 维数。

例如，在二维空间中，取函数组为：

$$f(\boldsymbol{x},\alpha)=\text{sign}\{\boldsymbol{w}\bullet\boldsymbol{x}+w_0\} \tag{4.5}$$

其中，sign{ }表示符号函数。

$$\text{sign}\{u\}=\begin{cases}+1, & \text{若}u\geqslant 0\\ -1, & \text{若}u<0\end{cases} \tag{4.6}$$

式(4.5)中的参数为 $\alpha=\{\boldsymbol{w},w_0\}$，该函数组就是这些参数取所有可能的值时在二维空间（平面）上得到的所有有向直线：

$$w_1x_1+w_2x_2+w_0=0 \qquad \forall \boldsymbol{w},w_0 \tag{4.7}$$

其中，任一条直线将平面分成两个半平面，直线的法线方向所对的半平面内的样本标记为+1，另外一个半平面内的样本标记为 –1。当 $l=2$ 时有 4 种分法。当 $l=3$ 时有 8 种分法，均可用式（4.7）中的有向直线分完，如图 4.2 和图 4.3 所示。当 $l=4$ 时有 16 种分法，图 4.4 给出了一个反例，式（4.7）中找不出一条直线能将其正确分类，因此函数组式（4.5）能分完的样本集最多只能包含 3 个样本点，该函数组的 VC 维数就是 3。

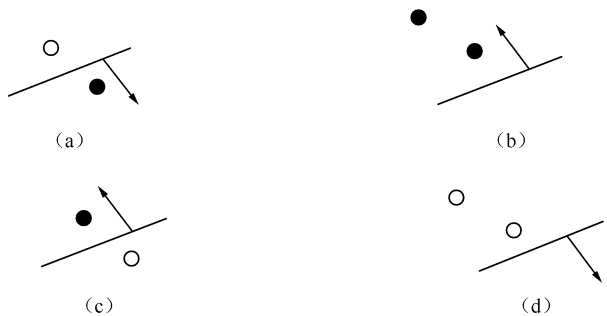


图 4.2　l=2 时的 VC 维数图解

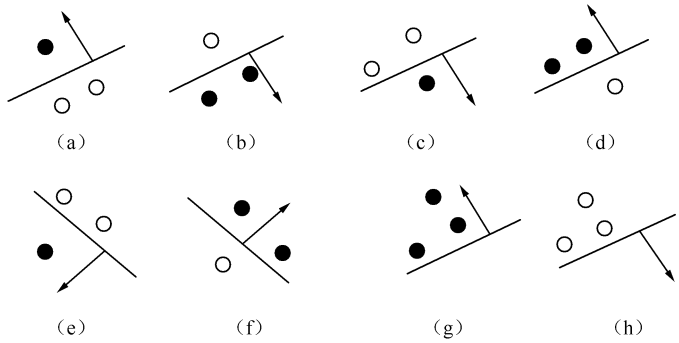


图 4.3　l=3 时的 VC 维数图解

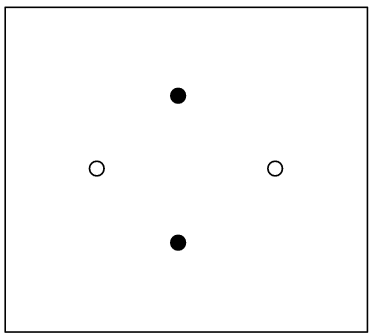


图 4.4　l=4 时的不可分情形

若对任意正整数 n，总存在一组 n 个矢量，能用该组指示函数按所有可能的 2^n 种方式分开，则该组指示函数的 VC 维数为无穷大。VC 维数有限是 ERM 归纳具有一致性并与概率分布无关的充分必要条件，同时也是快速收敛的充分条件。

上例的结果可推广到一般线性系统，线性指示函数：

$$f(\boldsymbol{x},\alpha)=\operatorname{sign}\left|\sum_{i=1}^{n}w_i x_i+w_0\right| \tag{4.8}$$

其 VC 维数 $h=n+1$。线性连续函数：

$$f(\boldsymbol{x},\alpha)=\sum_{i=1}^{n}w_i x_i+w_0 \tag{4.9}$$

的 VC 维数亦为 $h=n+1$，即对于线性模型，VC 维数与参数的数目一致。对于非线性系统，

VC 维数一般并不等于，还可能小于参数的数目，决定推广能力的是 VC 维数，而不是参数的数目的多少。对于一些比较复杂的机器学习（如神经网络），其 VC 维数除了与函数集（神经网络结构）有关外，还受学习算法等的影响，因而 VC 维数的确定更加困难。对于给定的学习函数集，如何计算 VC 维数是当前统计学理论中有待继续研究的问题。

4.2.2 推广性的界

统计学习理论系统地研究了各种类型的函数集（完全有界函数集、任意非正函数集和任意非负函数集）的经验风险和实际风险之间的关系，即推广性的界。得出的结论是：对于两类分类问题，对指示函数集中的所有函数（包括使经验风险最小的函数），经验风险 $R_{\text{emp}}(a)$ 和实际风险 $R(a)$ 之间以至少 $1-\eta$ 的概率满足如下关系：

$$R(a) \leqslant R_{\text{emp}}(a) + \sqrt{\left(\frac{h(\ln(2l/h)+l) - \ln(\eta/4)}{l}\right)} \tag{4.10}$$

其中，h 是函数集的 VC 维，l 是样本数。

这一结论从理论上说明了机器学习的实际风险是由两部分组成的：一是经验风险（训练误差，上式右边的第一部分）；另一部分称做置信范围（也称 VC 置信，上式右边的第二部分），它和机器学习的 VC 维及训练样本数有关。它反映了根据经验风险最小化原则得到的机器学习的推广能力，因此称为推广性的界。式（4.10）的关系可以简单表示为：

$$R(a) \leqslant R_{\text{emp}}(a) + \phi(l/h) \tag{4.11}$$

它表明，在有限训练样本下，机器学习的 VC 维越高（复杂性越高）则置信范围越大，导致真实风险与经验风险之间可能的差别越大。这就是为什么会出现过学习现象的原因，机器学习过程不但要使经验风险最小，还要使 VC 维尽量小以缩小置信范围，这样才能取得较小的实际风险，即对未来样本有较好的推广性。

4.2.3 结构风险最小化理论

从上面的结论看到，经验风险最小化原则在样本有限时是不合理的，因为我们需要同时最小化经验风险和置信范围。事实上，在传统方法如神经网络设计中，选择学习模型和算法的过程就是调整置信范围的过程，如果模型比较适合现有的训练样本（相当于 l/h 值），则可以取得比较好的效果。但因为缺乏理论指导，这种选择只能依赖先验知识和经验，造成了网络设计对使用者“技巧”的过分依赖。有了式（4.9）的理论依据，统计学习理论提出了一种

新的策略，即把函数集构造为一个函数子集序列，使各个子集按照 VC 维的大小（亦即 h 的大小）排列；在每个子集中寻找最小经验风险，在子集间折中考虑经验风险和置信范围，取得实际风险的最小。这种思想称做结构风险最小化（Structural Risk Minimization），即 SRM 原则[7]。

经验风险最小化的具体过程就是首先把函数集 $S=\{F(\boldsymbol{x},\alpha),\alpha\}$，$\alpha\in\Lambda$ 分解为一个函数子集序列（或叫子集结构）：

$$S_1\subset S_2\subset\cdots\subset S_k\subset\cdots\subset S \tag{4.12}$$

使各个子集能按照式（4.12）的大小排列，也就是按照 VC 维的大小排列，即

$$h_1\leqslant h_2\leqslant\cdots \tag{4.13}$$

这样在同一个子集中置信范围就相同；然后在每一个子集中寻找最小经验风险，通常它随着子集复杂性的增加而减小。选择最小经验风险与置信范围之和最小的子集，就可以达到期望风险的最小，这个子集中使经验风险最小的函数就是要求的最优函数。这种思想称为有序风险最小化或者结构风险最小化（Structural Risk Minimization ,SRM）原则，如图 4.5 所示。

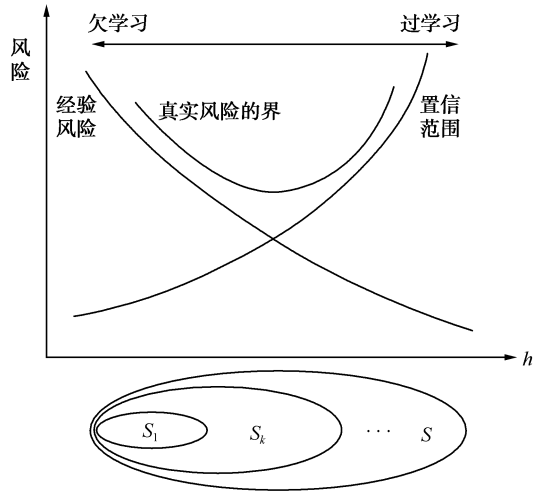


图 4.5　结构风险最小化原理图解

实现结构风险最小化原则有两种截然不同的思路：一种思路是通过选择一个具有适当结构的机器学习，保持置信范围固定不变，最小化经验风险，从而最小化期望风险；第二种思路恰好与第一种做法相反，这里保持经验风险固定，从而最小化置信范围，即设计函数集的某种结构使得在每个子集中都能取得最小的经验风险（如使训练误差为 0），然后只需从中选择适当的子集使置信范围最小，那么在这个子集中使置信范围最小的函数就是最优函数。实现这两种思路的机器学习分别是神经网络（第一种思路）和 SVM（第二种思路）。在使用

神经网络处理问题时，首先选定神经网络的结构，这就决定了神经网络的 VC 维，然后训练神经网络，使经验风险最小化。但由于目前神经网络结构选取并没有理论指导，而且通用的后向传播（Back Propagation, BP）学习算法容易陷入局部极小点，经验风险不能达到最小，所以神经网络的推广能力不能得到很好的控制。SVM 由有限训练样本得到的决策规则对独立的测试集仍然能够得到小的误差，是一种比较好的实现了结构风险最小化思想和 VC 维理论算法的方法。即先选择使置信范围最小的子集即支持向量，然后在其中构造最优函数。统计学习理论之所以从 20 世纪 90 年代以来受到越来越多的重视，很大程度上是因为它发展出了支持向量机这一通用学习方法。

4.3 支持向量机的工作原理

统计学习理论专门研究实际应用中有限样本情况的机器学习规律，并发展了支持向量机（Support Vector Machine，SVM）[8]这一新的通用学习方法，由于它基于结构风险最小化（SRM）原理，而不是传统统计学的经验风险最小化（ERM），因此，表现出很多优于已有方法的性能，迅速引起各领域的注意和研究兴趣，取得了大量的应用研究成果，推动了各领域的发展。

支持向量机的出色之处在于，其根据有限的样本信息在模型的复杂性（即对特定训练样本的学习精度，Accuracy）和学习能力（即无错误地识别任意样本的能力）之间寻求最佳折中，以期获得最好的推广能力（Generalization Ability）。

支持向量机的理论基础包括：

（1）VC 维理论不仅要使机器学习的经验误差最小，而且应该最小化函数集的 VC 维来控制学习机的结构误差，以达到 SVM 分类器具有较强的泛化能力的目的，即由有限的训练样本分类得到小的误差能够保证对独立测试集仍保持较小误差，解决了有限样本的“过学习”问题。

（2）引入最优超平面概念，使函数的 VC 维上界达到最小，而最优超平面问题可转化为二次规划问题。

（3）核空间理论通过非线性映射将输入空间映射到高维特征空间，使低维输入空间线性不可分问题转化为高维特征空间线性可分问题，且引入核函数从而绕过了高维空间，使运算在低维输入空间进行，从而不用确切知道非线性映射的具体形式。

4.3.1 最优分类面

支持向量机方法是从线性可分情况下的最优分类面发展而来的，基本思想可用图 4.6 的

两类待分类样本说明。圆与三角形符号分别代表两类不同的样本，假如这两类样本是线性可分的。待分类的样本集为：$\{\boldsymbol{x}_i, y_i\}, i=1,\cdots,N, y_i \in \{-1,+1\}, \boldsymbol{x}_i \in \mathbf{R}^d$，样本为 d 维向量，$y \in \{+1,-1\}$ 属于类别号。H_1、H_2 分别为各类中离分类超平面最近的样本且平行于分类超平面的平面，它们之间的距离叫做分类间隔（Margin）。则 SVM 学习的结果就是找到一个最优分类超平面，不仅能够将这两类样本分开，且分类间隙最大。在分类面上的样本为支持向量，从某种程度上来说，是样本中少量的支持向量决定了最优分类超平面。

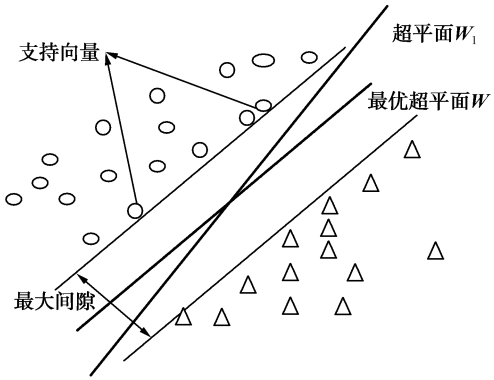


图 4.6　最优分类面

对于给定的数据集 $\{\boldsymbol{x}_i, y_i\}, i=1,\cdots,N, y_i \in \{-1,+1\}, \boldsymbol{x}_i \in \mathbf{R}^d$，分类的目的就是寻求 $(\boldsymbol{w}, b)$，最佳分离两类数据。若超平面 $\boldsymbol{w}\bullet\boldsymbol{x}+b$ 能将训练样本分开。则有：

$$\begin{cases} \boldsymbol{w}\bullet\boldsymbol{x}_i + b > 1, \text{若} y_i = 1 \\ \boldsymbol{w}\bullet\boldsymbol{x}_i + b < -1, \text{若} y_i = -1 \end{cases} \tag{4.14}$$

$$y_i[(\boldsymbol{w}\bullet\boldsymbol{x}_i)+b]-1 \geqslant 0, i=1,2,\cdots,N \tag{4.15}$$

分界面 $\boldsymbol{w}\bullet\boldsymbol{x}+b$ 的分类间隔为：

$$d(\boldsymbol{w},b) = \min_{\{x_i/y_i=1\}} \frac{\boldsymbol{w}\bullet\boldsymbol{x}_i+b}{|\boldsymbol{w}|} - \max_{\{x_i/y_i=-1\}} \frac{\boldsymbol{w}\bullet\boldsymbol{x}_i+b}{|\boldsymbol{w}|} \tag{4.16}$$

由式（4.13），式（4.14）可得：

$$d(\boldsymbol{w},b)=\frac{1}{|\boldsymbol{w}|}-\frac{-1}{|\boldsymbol{w}|}=\frac{2}{|\boldsymbol{w}|} \tag{4.17}$$

此时的分类间隔等于$2/|\boldsymbol{w}|$，要使分类间隔最大，等价于使$\|\boldsymbol{w}\|^2/2$最小。满足式（4.13），且使$\frac{1}{2}\|\boldsymbol{w}\|^2$最小的分类面为最优分类超平面。使分类间隔最大实际上就是对推广能力的控制，这是 SVM 核心思想之一。统计学习理论指出，在 N 维空间中，设样本分布在一个半径为 R 的超球范围内，则满足条件$\|\boldsymbol{w}\|^2 \leqslant A$ 的正则超平面构成的指示函数集 $f(\boldsymbol{x},\boldsymbol{w},b)=\mathrm{sgn}(\boldsymbol{w}^{\mathrm{T}}\boldsymbol{x}+b)$（sgn() 为符号函数）的 VC 维满足下面的界。

$$h \leqslant \min([R^2A^2],N)+1 \tag{4.18}$$

因此，使$\|\boldsymbol{w}\|^2$最小就是使 VC 维的上界最小，实现了 SRM 准则中对函数复杂性的选择。引入拉格朗日泛函形式：

$$l(\boldsymbol{w},b,a)=\frac{1}{2}\|\boldsymbol{w}\|^2-\sum_{i=1}^{N}a_i\left[y_i(\boldsymbol{w}\bullet\boldsymbol{x}_i+b)-1\right] \tag{4.19}$$

a_i 是拉格朗日因子，对 $\boldsymbol{w}$,b 求 Largrang 函数的极小值。由于上述问题是一个凸二次规划（Quadratic Programming，QP）问题，可以把原问题转化为对偶问题，由满足最优解的条件得：

$$\frac{\partial l(\boldsymbol{w},b,a)}{\partial b}=0 \Rightarrow \sum_{i=1}^{N}a_i^*y_i=0 \tag{4.20}$$

$$\frac{\partial l(\boldsymbol{w},b,a)}{\partial \boldsymbol{w}}=0 \Rightarrow \boldsymbol{w}^*=\sum_{i=1}^{N}a_i^*\boldsymbol{x}_iy_i \tag{4.21}$$

对 a_i 求解下列函数的最大值：

$$\max W(a)=\max_a\{\min_{\boldsymbol{w},b} l(\boldsymbol{w},b,a)\}=\max_a\{\sum_{i=1}^{N}a_i-\frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N}a_ia_jy_iy_j(\boldsymbol{x}_i\bullet\boldsymbol{x}_j)\} \tag{4.22}$$

求得解 a_i^*，通常只有少部分 a_i^* 不为零，对应的样本就是支持向量。得到最优分类函数是：

$$f(x)=\mathrm{sgn}\{(\boldsymbol{w}^*\bullet\boldsymbol{x})+b^*\}=\mathrm{sgn}\{\sum_{i=1}^{N}a_i^*y_i(\boldsymbol{x}_i\bullet\boldsymbol{x})+b\} \tag{4.23}$$

b 是分类阈值，可以用任一个支持向量式（满足式（4.14）中的等号）求得，或通过两类中任意一对支持向量取中值求得。

4.3.2　广义最优分类面

在线性不可分的情况下，有一些样本不能被超平面正确分类，为使数据在线性不可分的情况下构造最优超平面，可在条件式（4.14）中增加一个松弛项 $\xi_i \geqslant 0$，成为：

$$y_i[(\boldsymbol{w} \bullet \boldsymbol{x}_i) + b] \geqslant 1 - \xi_i, \quad i = 1, 2, \cdots, N \tag{4.24}$$

对于足够小的 $\sigma > 0$，只要使下式：

$$F_\sigma(\xi) = \sum_{i=1}^{N} \xi_i^\sigma \tag{4.25}$$

最小，就可以使错分样本数量最小，对应线性可分情况下使分类间隔最大，在线性不可分情况下可引入约束条件：

$$\|\boldsymbol{w}\|^2 \leqslant c_k \tag{4.26}$$

在约束条件式（4.23）、式（4.25）下，对式（4.24）求最小值，就得到了线性不可分情况下的最优分类面，称其为广义最优分类面。在满足条件式（4.23）时，最优问题转化为下列函数的极小值：

$$\min_{\boldsymbol{w}, b, \xi} \frac{1}{2}\|\boldsymbol{w}\|^2 + C\left(\sum_{i=1}^{N} \xi_i\right) \tag{4.27}$$

前一项反映的是置信范围，后一项反映的是训练误差，前后两项体现了结构风险最小化原则。其中 C 为惩罚因子，它实际上控制对错分样本惩罚的程度，反映了我们对错误划分的重视程度，C 越大对错误的惩罚越重。用解最优分类超平面时同样的方法求解这一优化问题，同样得到一个二次函数极值问题，只是受限条件为 $0 \leqslant a_i \leqslant C$，$i = 1, 2, \cdots, N$，即约束条件：

$$\sum_{i=1}^{N} a_i y_i = 0 \tag{4.28}$$

$$0 \leqslant a_i \leqslant C, i = 1, 2, \cdots, N \tag{4.29}$$

在式（4.27）和式（4.28）的约束条件下，求解下列函数的最大值：

$$\max_a \left\{\sum_{i=1}^{N} a_i - \frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} a_i a_j y_i y_j (\boldsymbol{x}_i \bullet \boldsymbol{x}_j)\right\} \tag{4.30}$$

4.3.3　核函数

对于线性不可分问题，可以通过引入松弛变量和惩罚函数的方法推广最优超平面的概念。

更一般的方法是通过核函数[9,10]将输入空间中的样本通过某种非线性函数关系映射到一个特征空间中，即 $\phi:\mathbf{R}^d \to F$。使待分类样本在此特征空间（高维空间）线性可分，并在此特征空间求最优分类面，如图 4.7 所示。

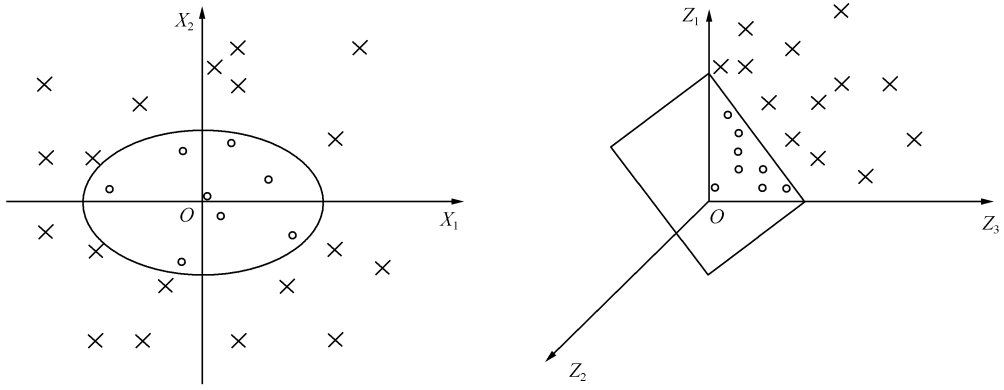


图 4.7　核函数原理图

图 4.7 中左图表示平面上的非线性分类问题，不妨假定分类器已知，且是二次函数并可表示成形式 $ax_1^2 + bx_1x_2 + cx_2^2 = d$ ，做变换：

$$F:\mathbf{R}^2 \to \mathbf{R}^3, F(x_1,x_2) = (x_1^2, x_1x_2, x_2^2)$$

显然，平面上的二次曲线 $ax_1^2 + bx_1x_2 + cx_2^2 = d$ 被 F 变换成 $\mathbf{R}^3$ 的平面 $az_1 + bz_2 + cz_3 = d$ 。由此，我们可以想象平面上的任意多项式分类器曲线可变换成适当高维空间的超平面，并且此超平面分离变换后的样本集，即我们可将任一非线性分类问题通过特征映射转变为高维特征空间的线性可分问题，因此超平面的系数可由特征空间的最大边缘算法求出。由图 4.7 可以看出，当平面上的分类是高次多项式时，特征空间的维数会相当高，直接在特征空间使用最大边缘算法去计算代价太大甚至无法实现。注意到平面上的最大边缘算法仅与 $\langle x,y\rangle$ 有关，其中 $x = \langle x_1, x_2\rangle$， $y = \langle y_1, y_2\rangle$，因此特征空间的最大边缘算法只与 $\langle F(x), F(y)\rangle$ 有关。为了减少计算量，针对上面的特征映射，实际使用中，我们将其修正为:

$$F_1:\mathbf{R}^2 \to \mathbf{R}^3, F_1(x_1,x_2) = (x_1^2, \text{sqrt}(2)x_1x_2, x_2^2)$$

这样可得到简单核 $K(x,y) = (\langle x,y\rangle)^2$，与由 F 得到的核相比，它的计算量较小。由上面的分析还可以看出，定义核函数只是为了替换 SVM 优化问题的内积，核函数的重要性应体现在减少计算量上，它与线性可分性并无直接的关系，而简单的核函数可以通过适当修正特征函数得到。

常用的核函数有以下四种形式。

（1）线性核函数：

$$K(\boldsymbol{x},\boldsymbol{x}_i)=\boldsymbol{x}^{\mathrm{T}}\boldsymbol{x}_i$$

（2）多项式核函数：

$$K(\boldsymbol{x},\boldsymbol{x}_i)=(\boldsymbol{x}\bullet\boldsymbol{x}_i+1)^q$$

（3）径向基函数（RBF）：

$$K(\boldsymbol{x},\boldsymbol{x}_i)=\exp(-\|\boldsymbol{x}-\boldsymbol{x}_i\|^2/2\sigma^2)$$

（4）Sigmoid 函数：

$$K(\boldsymbol{x},\boldsymbol{x}_i)=\tanh(v(\boldsymbol{x}\bullet\boldsymbol{x}_i)+c)$$

核函数对分类器的性能有重要影响，因此如何去构造、选择核函数及参数成为人们关注的问题。对于 RBF 核函数分类器，它与传统 RBF 方法的重要区别是：这里每个基函数中心对应一个支持向量，它们及输出权值都是由算法自动确定的。对于 Sigmoid 函数构成的分类器，可以把它看成一个特殊类型的两层 Sigmoid 神经网络，但其结构（权数目）是由 SVM 训练来自动决定的，而且算法不会产生局部极小点问题。

在构建分类器的时候，我们首先需要确定核函数的类型，然后对参数 C 和核函数参数进行选择。对于四种基本的核函数，RBF 函数往往是最先被考虑的，它是比较可靠的。

4.4　支持向量机的训练法[11]

支持向量机的最终求解问题归结为一个有约束的二次规划（Quadratic Programming,QP）问题。具体形式如下。

分类 SVM：

$$\min_{\boldsymbol{a}}\frac{1}{2}\boldsymbol{a}^{\mathrm{T}}\boldsymbol{Q}\boldsymbol{a}-\boldsymbol{e}^{\mathrm{T}}\boldsymbol{a} \tag{4.31}$$

约束条件：

$$\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{a}=0,0\leqslant a_i\leqslant C \tag{4.32}$$

回归 SVM：

$$\min_{\boldsymbol{a}^*,\boldsymbol{a}}\frac{1}{2}[\boldsymbol{a}^{\mathrm{T}},(\boldsymbol{a}^*)^{\mathrm{T}}]\begin{pmatrix}\boldsymbol{Q}&-\boldsymbol{Q}\\-\boldsymbol{Q}&\boldsymbol{Q}\end{pmatrix}\begin{pmatrix}\boldsymbol{a}\\\boldsymbol{a}^*\end{pmatrix}+[\varepsilon\boldsymbol{e}^{\mathrm{T}}+\boldsymbol{y}^{\mathrm{T}},\varepsilon\boldsymbol{e}^{\mathrm{T}}-\boldsymbol{y}^{\mathrm{T}}]\begin{pmatrix}\boldsymbol{a}\\\boldsymbol{a}^*\end{pmatrix} \tag{4.33}$$

约束条件：

$$[\boldsymbol{e}^{\mathrm{T}}, -\boldsymbol{e}^{\mathrm{T}}]\begin{pmatrix}\boldsymbol{a}\\ \boldsymbol{a}^{*}\end{pmatrix} = 0, 0 \leqslant \boldsymbol{a}, \boldsymbol{a}^{*} \leqslant C \tag{4.34}$$

对上面的优化问题，可用传统的标准二次型优化技术来求解这个优化问题，如牛顿法、共轭梯度法、内点法等。但是，这些方法的运算速度是非常慢的，且还存在着稳定性问题。产生这个问题的主要原因是：首先，QP 方法需要计算和存储核函数矩阵，当样本点数目较大时，需很大的内存。例如，当样本点数目超过 4000 时，存储核函数矩阵需要高达 128MB 内存。其次，SVM 在二次型寻优过程中要进行大量的矩阵运算，多数情况下，寻优算法是占用算法时间的主要部分；另外，QP 方法是一般的优化方法，并没有利用 SVM 对偶优化问题的具体特性，如核矩阵的稀疏性、对称性，约束条件为线性约束和矩阵约束。这种基于 QP 的 SVM 的训练方法只适合小样本和中等规模的样本场合。

为了减小 SVM 学习方法的计算复杂性，利用 SVM 优化问题本身所具有的特性，近年来已经提出了几种改进的支持向量机的训练算法。主要有 3 大种：以 SMO（Sequential Minimal Optimization ）为代表的分解算法；以 EG（Exponentiated Gradients Gradients）为代表的多变量更新算法；以 SOR(Successive Overrelaxation)为代表的序列方法。另外，还有许多学者改变了标准 SVM 的优化目标，把二次型优化问题转化为线性优化问题。下面将分别介绍各自的思想及优缺点。

4.4.1 分块算法

1995 年，Cortes 和 Vapnik 给出了一种求解支持向量机二次规划（QP）[12] 问题的分块算法。其依据是支持向量机的最终求解结果只与支持向量有关，与非支持向量无关。其实现过程是将初始 QP 问题分解为一系列小规模的 QP 子问题，不断地求解 QP 子问题，保留解中的支持向量，并加入到新的 QP 子问题中。每个 QP 子问题都采用上次求解的结果作为初始值。直到所有的 QP 子问题求解完毕。这种方法可以大大减小算法占用的系统内存。

第一类方法是所谓的“块算法”（Chunking Algorithm）[13]，它基于这样一个事实，即去掉 Lagrange 乘子等于零的训练样本不会影响原问题的解。对于给定的训练样本集，如果其中的支持向量是已知的，寻优算法就可以排除非支持向量，只需针对支持向量计算权值（即 Lagrange 乘子）即可。实际上，支持向量是未知的，因此“块算法”的目标就是通过某种迭代方式逐步排除非支持向量。具体的做法是：选择一部分样本构成工作样本集进行训练，剔除其中的非支持向量，并用训练结果对剩余样本进行检验，将不符合训练结果（一般是指违反 KKT 条件）的样本（或其中的一部分）与本次结果的支持向量合并为一个新的工作样本集，然后重新训练。如此重复直到获得最优结果为止。当支持向量的数目远远小于训练样本数目

时，“块算法”显然能够大大提高运算速度。然而，如果分类 SVM 是不可分的，或者是回归 SVM 的情况，这时的支持向量的数目本身就比较大，随着算法迭代次数的增多，工作样本集也会越来越大，算法依旧会变得十分复杂。

针对块算法的缺点，第二类方法把问题分解成为固定样本数的子问题：工作样本集的大小固定在算法速度可以容忍的限度内，迭代过程中只是将剩余样本中部分“情况最糟的样本”与工作样本集中的样本进行等量交换，即使支持向量的个数超过工作样本集的大小，也不改变工作样本集的规模，而只对支持向量中的一部分进行优化。以分类 SVM 为例，固定工作样本集的算法是，把训练样本分成两部分，一是工作集 W，一是保留集 R，重写二次规划问题可得：

$$\min_{\boldsymbol{a}_W} \frac{1}{2}[\boldsymbol{a}_W^{\mathrm{T}}, \boldsymbol{a}_R^{\mathrm{T}}]\begin{pmatrix} \boldsymbol{Q}_{WW} & -\boldsymbol{Q}_{WR} \\ -\boldsymbol{Q}_{RW} & \boldsymbol{Q}_{RR} \end{pmatrix}\begin{pmatrix} \boldsymbol{a}_W \\ \boldsymbol{a}_R \end{pmatrix} - \sum_{i\in W} a_i - \sum_{i\in R} a_i \tag{4.35}$$

$$\sum_{i\in W} y_i a_i + \sum_{i\in R} y_i a_i = 0, 0 \leqslant a_i \leqslant C \tag{4.36}$$

具体算法描述如下。

Step 1：给定一常数 $q \leqslant l$ 作为工作集的大小，设定优化变量初始值为 a^1，设定 k=1。

Step 2：如果 a^k 是优化问题式（4.30），式（4.31）的最优解，则停止程序，否则从训练样本集中选择一工作样本集，a_W^k 和 a_R^k 分别是工作集和保留集所对应的 Lagrange 常数,即优化变量。

Step 3：求解优化问题式（4.34），式（4.35），即求优化变量 a_W^{k+1}；

Step 4：设定 $a_R^{k+1} = a_R^k, k \leftarrow k+1$ 返回到 Step 2。

固定工作样本集的方法和块算法的主要区别在于：块算法的目标函数中仅包含当前工作样本集中的样本，而固定工作样本集方法虽然其优化变量仅包含工作样本，但其目标函数却包含整个训练样本集，即工作样本集之外的样本的 Lagrange 乘子固定为前一次迭代的结果，而不像块算法中那样设为 0。而且固定工作样本集方法还涉及一个确定换出样本的问题（因为换出的样本可能是支持向量）。这样，这一类算法的关键就在于找到一种合适的迭代策略，使得算法最终能收敛并且较快地收敛到最优结果。固定工作样本集算法的关键在于选择一种最优的工作集选择算法，一是它影响算法收敛性的理论分析，二是它影响算法的收敛速度。

对迭代算法来说，初始点的选择是很重要的，初始点对收敛速度有很大的影响。Marchlo 提出初始最优工作集的选择方法——GetBorder，其主要思想是这样的：认为两个类之间的相近点最有可能成为支持向量。第一步，对于一个类的所有训练矢量，在特征空间中寻找另一个类中与它最短距离的训练矢量，即图 4.8 中所描述的第一步；第二步，从一列最小距离中找出几个较小距离所对应的点，即图 4.8 中的第二步，然后把这些点作为初始工作集的选择点。

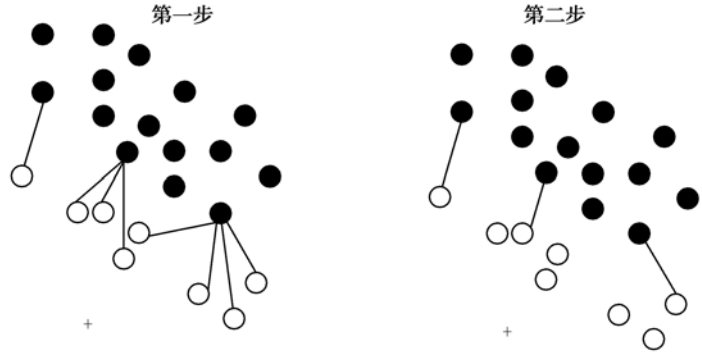


图 4.8 GetBorder 工作原理

当工作集中只有两个样本时，上述固定工作集方法就变成了 Platt 提出的著名的 SMO 算法[14]。该算法可以说是分解算法的一个极端特例，其优点是针对两个样本的二次规划问题可以有解析解的形式。因为只有两个变量，应用等式约束可以将其中一个用另一个表示出来，所以迭代过程中每一步的子问题的最优解可以直接用解析的方法求出。这样，算法避开了复杂的数值求解优化问题的过程；其工作集的选择也别具特色，不是传统的最陡下降法，而是启发式。Platt 设计了一个两层嵌套循环分别选择进入工作样本集的样本，在外环中寻找违背 KKT 最优条件的样本，然后在内环中再选择另一个样本，完成一次优化。再循环，进行下一次优化，直到全部样本都满足最优条件为止。这种启发式策略大大加快了算法的收敛速度。SMO 算法主要耗时在最优条件的判断上，所以应寻找最合理即计算代价最低的最优条件判别式，同时对常用的参数进行缓存。子问题的规模和迭代的次数是一对矛盾，SMO 将工作样本集的规模减少到 2，一个直接的结果就是迭代次数的增加。所以 SMO 实际上是将求解子问题的耗费转嫁到迭代上，然后再在迭代上寻求快速算法。但是，SMO 迭代策略的思想是可以用到其他迭代算法中的。可见，SMO 还有改进的余地。SMO 方法不仅能应用于标准的 SVM，而且还能应用于 SVM 的变种——最小二乘法 SVM（LS-SVM）中去，可见 SMO 算法具有一定的普适性。应该说，块算法和固定工作样本集算法各有优缺点。毫无疑问，固定工作样本集的算法解决了占用内存的问题，而且限制了子问题规模的无限增大。但是，从这个意义上来说，固定工作样本集的算法把解标准二次型的寻优问题的时间转嫁到循环迭代上了，它的迭代次数一般会比“块算法”多。尤其是 SMO，如果没有一个好的启发式迭代策略，该算法就是一种盲目的“爬山法”。

4.4.2　多变量更新算法

分解算法虽然取得了成功，大大减小了 SVM 学习算法的计算复杂性，但是这种算法的具体实施比较困难，具有相当的经验启发成分，尤其是工作集的选择和迭代策略的确定。为了克服这个难题，很多学者提出了多变量迭代更新算法，它不像分解算法一次迭代只更新工作集的学习系数一样，而是更新全部训练集的学习系数。

多变量更新算法基本上是基于梯度的方法。主要有两种方法：一种是投影梯度法；另一种是对数梯度法。Friess 提出类似于感知器的 Adatron 算法的 Kernel-ada-tron 算法，Lagrange 系数采用梯度法；Viiavummar 提出另外一种梯度算法，特点是将 SVM 原问题中的偏置 b 也看做系数。该方法的特点是原理简单，容易编程实现，但是梯度法的难点是学习率的大小难以确定，于是某些学者提出了对数梯度法（Exponentiated Gradients Gradients，EG）[15]。最初对数梯度法是由 Littlestone 提出并应用于 Winnow 上的，后来得到了详尽的研究。在这种方法里,学习参数的更新率是学习参数本身乘以一个常数，即：

$$a_i^{k+1} = a_i^k \bullet \beta \tag{4.37}$$

其中，β 是常数,而不是传统的梯度。

$$a_i^{k+1} = a_i^k + \Delta a_i^{k+1} \tag{4.38}$$

理论分析和试验结果都表明，当学习机的稀疏性较强时，对数梯度法（EG）比传统的加性梯度下降法（GD）具有更快的收敛速度，而 SVM 学习机恰好具有稀疏性。Nello Cristianini 和 Fei Sha 提出用 EG 来训练支持向量机，均取得了较好的效果。

4.4.3　序列算法

解决算法速度问题的另一个途径是采用序列优化的思想[16]。这种方法的主要目的是研究当出现新的单个样本时，它与原有样本集或其子集，或者与原有样本集训练结果之间有何种关系。例如，它的加入对原有样本集的支持向量有什么样的影响，怎样迅速地确定它对新的决策函数的贡献等。如果能够简单、有效地确定单个样本加入工作样本集后对训练结果的影响，那么当出现新的样本时，可以利用原来的训练结果而不必重新开始；也可以让训练样本逐个进入工作样本集以简化寻优过程，提高算法速度。这实际上是将工作样本集中的样本数减少到 1。这种算法也可以用于 SVM 的在线学习方法, Mangasarian 提出的 SOR（Successive Overrelaxation）方法就是这样一种思路，通过在原目标函数中加一项 b^2，从而对偶问题多了 1 项，而约束条件少了 1 项等式约束，变为边界约束条件下的二次规划问题，适合迭代求解。同时，应用矩阵分解技术，每次只需更新 Lagrange 乘子的 1 个分量，而不需将所有样本载入

内存，提高了收敛速度。Gert Cauwenberghs 提出了一种增量减量式序列学习方法，即增加 1 个训练样本或减少 1 个训练样本时对 Lagrange 系数和支持向量机的影响。实验表明，算法是有效的，特别是减少 1 个样本时，对模型选择算法 LOO（Leave One Out）的形象解释。Mario Martin 提出了回归 SVM 的在线序列学习方法，其思路和 Gert 是相同的。Liva Ralaivola 提出了一种增量式序列学习方法，它的特点是基于 RBF 核的局部特性只更新对学习机输出影响最大的 Lagrange 系数，其余的 Lagrange 系数不变，这样就可以减小计算复杂性。

4.5 小结

支持向量机与人工神经网络类似，都是机器学习方法，但与神经网络不同的是支持向量机使用的是数学方法和优化技术。支持向量机是一种新的非常有潜力的分类技术，是一种基于统计学习理论的模式识别方法，在解决小样本、非线性及高维模式识别问题中表现出许多良好的特性，并能够推广应用到函数拟合等其他机器学习问题中，现在已经在许多领域取得了成功的应用[17]。

支持向量机的关键在于核函数的选取。由于低维空间的向量集难分类，通常的解决方法是将它们映射到高维空间，但这种方法带来的困难是计算复杂度的增加。而核函数可以较好地解决这个问题。只要选用适当的核函数，就可以得到高维空间的分类函数。在支持向量机理论中，采用不同的核函数将导致不同的支持向量机算法。

虽然支持向量机的应用领域日趋广泛，但是它在处理大规模问题时仍然存在许多局限性：①由于支持向量机的训练过程实质是求解一个二次规划问题,其求解时间复杂度为 $O(N^3)$，空间复杂度为 $O(N^3)$。当训练集规模巨大时，会导致支持向量机的训练时间太长和内存空间不足等问题。②支持向量机的训练结果是用支持向量表示的，当支持向量数目太大时，会超出内存限制，使得分类器不能全部装入内存，影响分类器的使用。③由于计算机系统的不可靠性，集中表示的分类器会面临失效的严重风险。④二次规划问题的求解过程本质是面向批量数据，已经训练好的支持向量机无法将新增加的训练样本纳入。

在支持向量机理论的研究中，鲁棒性问题是一个值得关注的课题。如何将神经网络、模糊逻辑等领域内已有的研究思想和方法与支持向量机理论相结合，提出更新、更有效的方法仍然是支持向量机理论的研究重点之一。此外，有限维空间的支持向量机理论发展较快，但无限维空间的支持向量机理论还需深入研究。

参 考 文 献

[1] 李国正，王猛，曾华军译．支持向量机导论．北京：电子工业出版社，2004．
[2] 王珏，周志华，周傲英. 机器学习及其应用. 北京：清华大学出版社，2006．
[3] 边肇祺，张学工等．模式识别．北京：清华大学出版社，2000．
[4] Vladimir N.Vapnik，许建华译．统计学习理论．北京：电子工业出版社，2004．
[5] Vladimir N.Vapnik. The Nature of Statistical Learning Theory. New York: Spring-Verlag, 2004．
[6] BURGES C J C. A Tutorial on Support Vector Machines for Pattern Recognition. Data Mining and Knowledge Discovery, 2001, 2(2)：121-167．
[7] 王磊．支持向量机学习算法的若干问题研究. 电子科技大学硕士学位论文，2007．
[8] Yuh-Jye Lee,Su-Yun Huang. Reduced Support Vector Machines: A Statistical Theory. IEEE transactions on neural networks, 2007, 18(1):1-13．
[9] J. Yang, A. F. Frangi, et al. KPCA plus LDA: A Complete Kernel Fisher Discriminant Framework for Feature Extraction and Recognition. IEEE Trans. Pattern Anal. Mach. Intel, 2005, 27(2): 230-244.
[10] Yuh-Jye Lee, Olvi. L. Mangasarian. RSVM: Reduced support vector machines. in Proc. 1st SIAM Int. Conf. Data Mining, 2001．
[11] V N Vapnik .Statistical learning theory. New York: John Wiley and Sons , Inc , 1998．
[12] Zhe Wang, Songcan Chen. New Least Squares Support Vector Machines Based on Matrix Patterns. Neural Processing Letters, 2007, 26(1): 41-56．
[13] Corinna Cortes, Vladimir Vapnik. Support-Vector Networks. Machine Learning, 1995, 20(3): 273-297．
[14] John C. Platt. Sequential Minimal Optimization: A Fast Algorithm for Training Support Vector Machines. Microsoft Research. Technical Report (MSR-TR-98-14), April 21, 1998．
[15] Jyrki Kivinen, Manfred K. Warmuth. Exponentiated Gradient versus Gradient Descent for Linear Predictors. Information and Computation, 1997,132(1):1-63．
[16] 王婷．支持向量机的序列最小优化学习算法研究．山东大学硕士学位论文，2006．
[17] 骆瑞玲．基于 SVM 的与文本无关的说话人识别算法研究．兰州理工大学硕士学位论文，2006．

Chapter 5

第5章 遗传算法

按照达尔文的进化论，地球上的每一物种从诞生开始就进入了漫长的进化历程。通过对生物进化机理的研究，充分证明了生物种群的生存过程普遍遵循“自然选择、适者生存”的进化准则。

种群中的个体根据对环境的适应能力而被大自然所选择或淘汰。进化过程的结果反映在个体结构上，遗传物质以基因的形式排列在染色体上，每个基因有特殊的位置并控制生物的某些特性。在一定的环境影响下，生物物种通过自然选择、基因交换和变异等过程进行繁殖生长，构成了生物的整个进化过程。

在生物的整个进化过程中，生物种群不断地完善和发展。可见，生物进化过程本质上是一种优化过程，在计算机科学上具有直接的借鉴意义。在计算机技术迅猛发展的时代，生物进化过程不仅可以在计算机上模拟实现，而且还可以模拟进化过程，创立新的优化计算方法，并应用到复杂工程领域中，这就是遗传算法等一类模拟自然进化计算方法的思想源泉。以生物进化过程为基础，计算科学学者提出了各种模拟形式的计算方法。

一般认为，进化计算包括三个组成部分：由美国密歇根大学的 John H.Holland 教授提出的遗传算法[1]；由美国科学家 Lawrence J.Fogel 等人提出的进化规划[2,3]；由德国科学家 Ingo Rechenberg 和 Hans-Paul Schwefel[4]提出的进化策略。他们用不同的进化控制模式模拟了生物进化过程，从而形成了三种具有普遍影响的模拟进化的优化计算方法。这三种方法统称为进化计算。

遗传算法（Genetic Algorithm，GA），是进化计算的一个部分，是模拟达尔文的遗传选择和自然淘汰的生物进化过程的计算模型，是一种通过模拟自然进化过程搜索最优解的方法。它是由美国 Michigan 大学的 J.Holland 教授于 1975 年首先提出来的，在出版了颇有影响的专著《Adaptation in Natural and Artificial Systems》之后，GA 这个名称才逐渐为人所知。

5.1　遗传算法概述

遗传算法是一类借鉴生物界自然选择和自然遗传机制的随机化搜索算法。它简单、通用，鲁棒性强，适于并行处理，因此在过去的 30 多年中，遗传算法已取得了成功的应用，受到了人们的广泛关注。在机器学习、软件技术、图像处理、模式识别、神经网络、工业优化控制、生物学、遗传学、社会科学等方面，显示了非常广泛的应用前景。

5.1.1　遗传算法的发展

1967 年，Holland 的学生 J.D.Bagley 在博士论文中首次提出“遗传算法（Genetic Algorithms）”一词。此后，Holland 指导学生完成了多篇有关遗传算法研究的论文。1975 年是遗传算法研究历史上十分重要的一年。这一年 Holland 出版了他的专著《自然系统和人工系统的自适应》（Adaptation in Natural and Artificial Systems），这是第一本系统论述遗传算法的专著，因此有人把 1975 年作为遗传算法的诞生年。Holland 在该书中系统地阐述了遗传算法的基本理论和方法，并提出了对遗传算法的理论研究和发展极其重要的模式理论（Schema Theory）。该理论首次确认了结构重组遗传操作对于获得隐含并行性的重要性。同年，K.A.De Jong 完成了他的博士论文《一类遗传自适应系统的行为分析》（An Analysis of the Behavior of a Class of Genetic Adaptive System）[5]。该论文所做的研究工作，可看做是遗传算法发展进程中的一个里程碑。这是因为他把 Holland 的模式理论与他的计算实验结合了起来，并将选择、交叉和变异操作进一步完善和系统化，同时又提出了诸如代沟（Generation Gap）等新的遗传操作技术。可以认为，De Jong 的研究工作为遗传算法及其应用打下了坚实的基础，他所得出的许多结论，迄今仍具有普遍的指导意义。

进入 20 世纪 80 年代，遗传算法迎来了兴盛发展时期，无论是在理论研究还是应用研究中都成了十分热门的课题。1985 年，在美国召开了第一届遗传算法国际会议（International Conference on Genetic Algorithms，ICGA），并且成立了国际遗传算法学会（International Society of Genetic Algorithms，ISGA），以后每两年举行一次。1989 年，Holland 的学生 D.E.Goldberg 出版了专著《搜索、优化和机器学习中的遗传算法》（Genetic

Algorithms in Search , Optimization, and Machine Learning）[6]，该书总结了遗传算法研究的主要成果，对遗传算法及其应用做了全面而系统的论述。

进入 20 世纪 90 年代，尤其是遗传算法的应用研究显得格外活跃，不但它的应用领域扩大，而且利用遗传算法进行优化和规则学习的能力也显著提高，同时产业应用方面的研究也在摸索之中。此外一些新的理论和方法在应用研究中亦得到了迅速的发展，这些无疑给遗传算法增添了新的活力。遗传算法的应用研究已从初期的组合优化求解扩展到了许多更新、更工程化的应用方面。

随着应用领域的扩展，遗传算法的研究出现了几个引人注目的新动向：一是基于遗传算法的机器学习，这一新的研究课题把遗传算法从历来离散的搜索空间的优化搜索算法扩展到具有独特的规则生成功能的崭新的机器学习算法。这一新的学习机制对于解决人工智能中知识获取和知识优化精炼的瓶颈难题带来了希望。二是遗传算法正日益和神经网络、模糊推理及混沌理论等其他智能计算方法相互渗透和结合，这对开拓 21 世纪新的智能计算技术将具有重要的意义。三是并行处理的遗传算法的研究十分活跃。这一研究不仅对遗传算法本身的发展，而且对于新一代智能计算机体系结构的研究都是十分重要的。四是遗传算法和另一个称为人工生命的崭新研究领域正不断渗透。所谓人工生命即用计算机模拟自然界丰富多彩的生命现象，其中生物的自适应、进化、免疫等现象是人工生命的重要研究对象，而遗传算法在这方面将会发挥一定的作用。五是遗传算法和进化规划（Evolution Programming，EP）及进化策略（Evolution Strategy，ES）等进化计算理论日益结合。EP 和 ES 几乎是和遗传算法同时独立发展起来的，同遗传算法一样，它们也是模拟自然界生物进化机制的智能计算方法，即同遗传算法具有相同之处，但也有各自的特点。目前，这三者之间的比较研究和彼此结合的探讨已形成热点。

在欧洲，从 1990 年开始每隔一年举办一次 Parallel Problem Solving from Nature 学术会议，其中遗传算法是会议主要内容之一。此外，以遗传算法的理论基础为中心的学术会议还有 Foundations of Genetic Algorithms，该会也是从 1990 年开始隔年召开一次。这些国际会议论文，集中反映了遗传算法近些年来的最新发展和动向。1991 年，L.Davis 编辑出版了《遗传算法手册》（Handbook of Genetic Algorithms）[7]，其中包括了遗传算法在工程技术和社会生活中的大量应用实例。1992 年，Koza 发表了他的专著《遗传程序设计：基于自然选择法则的计算机程序设计》[8]。1994 年，他又出版了《遗传程序设计第二册：可重用程序的自动发现》[9]，深化了遗传程序设计的研究，使程序设计自动化展现了新局面。

国内也有不少的专家和学者对遗传算法基本理论进行了改进。2002 年，戴晓明等人[10]应用多种群遗传并行进化的思想，对不同种群基于不同的遗传策略，如变异概率、不同的变异算子等来搜索变量空间，并利用种群间迁移算子来进行遗传信息交流，以解决经典遗传算法的收敛到局部最优值问题。2004 年，赵宏立等人[11]针对简单遗传算法在较大规模组合优化问

题上搜索效率不高的现象，提出了一种用基因块编码的并行遗传算法（Building-block Coded Parallel GA，BCPGA）。该方法以粗粒度并行遗传算法为基本框架，在染色体群体中识别出可能的基因块，然后用基因块作为新的基因单位对染色体重新编码，产生长度较短的染色体，再用重新编码的染色体群体作为下一轮以相同方式演化的初始群体。2005年，江雷等人[12]针对并行遗传算法求解 TSP 问题，探讨了使用弹性策略来维持群体的多样性，使得算法跨过局部收敛的障碍，向全局最优方向进化。

有关遗传算法的学术论文也不断在《Artificial Intelligence》、《Machine Learning》、《Information Science》、《Parallel Computing》、《Genetic Programming and Evolvable Machines》、《IEEE Transactions on Neural Networks》、《IEEE Transactions on Signal Processing》等杂志上发表。1993 年，MIT 出版社创刊了新杂志《Evolutionary Computation》。1997 年，IEEE 又创刊了《Transactions on Evolutionary Computation》。《Advanced Computational Intelligence》由模糊集合创始人 L.A.Zadeh 教授为名誉主编。目前，关于遗传算法研究的热潮仍在持续，越来越多的从事不同领域的研究人员已经或正在置身于有关遗传算法的研究或应用之中。

5.1.2　遗传算法的特点和应用

遗传算法是一类可用于复杂系统优化的具有鲁棒性的搜索算法，与传统的优化算法相比，主要有以下特点[13]。

（1）遗传算法以决策变量的编码作为运算对象。传统的优化算法往往直接利用决策变量的实际值本身来进行优化计算，但遗传算法不是直接以决策变量的值，而是以决策变量的某种形式的编码为运算对象。这种对决策变量的编码处理方式，使得我们在优化计算过程中可以借鉴生物学中染色体和基因等概念，可以模仿自然界中生物的遗传和进化机理，也使得我们能够方便地应用遗传操作算子。

（2）遗传算法直接以适应度作为搜索信息，无需其他辅助信息。传统的优化算法不仅需要利用目标函数值，而且搜索过程往往受目标函数的连续性约束，还可能需满足目标函数导数必须存在的要求以确定搜索方向。而遗传算法仅使用由目标函数值变换来的适应度函数值，就可确定进一步的搜索范围，无需目标函数的导数值等其他一些辅助信息。对于很多目标函数无法求导、很难求导或导数不存在的优化问题及组合优化问题等，应用遗传算法就显得比较方便，因为它避开了函数求导数的障碍。此外，直接利用目标函数值或个体适应度，也可以使我们把搜索范围集中到适应度较高的部分搜索空间中，从而提高搜索效率。

（3）遗传算法使用多个点的搜索信息，具有隐含并行性。传统的优化算法往往是从解空间的一个初始点开始最优解的迭代搜索过程。单个搜索点所提供的搜索信息毕竟不多，所以搜索效率不高，有时甚至使搜索过程陷于局部最优解而停滞不前。遗传算法从由很多个体组

成的一个初始群体开始最优解的搜索过程，而不是从单个个体开始搜索。对这个群体所进行的选择、交叉、变异等运算，产生出新一代群体，其中包括了很多群体信息。这些信息可以避免搜索一些不必搜索的点，从而避免陷入局部最优，逐步逼近全局最优解。这是遗传算法所特有的一种隐含并行性。

（4）遗传算法使用概率搜索技术，而非确定性规则。很多传统的优化算法往往使用确定性的搜索方法，一个搜索点到另一个搜索点的转移有确定的转移方向和转移关系，这种确定性往往也有可能使得搜索达不到最优点，因此限制了算法的应用范围。而遗传算法是一种自适应搜索技术，其选择、交叉、变异等运算都是以一种概率方式来进行的，从而增加了搜索过程的灵活性，同时能以很大的概率收敛于最优解，具有较好的全局优化求解能力。当然，交叉概率、变异概率等参数也会影响算法的搜索效果和搜索效率，所以如何选择遗传算法的参数在其应用中是一个比较重要的问题。另外，与其他一些算法相比，遗传算法的鲁棒性又会使参数对其搜索效果的影响尽可能的低。

由于遗传算法的整体搜索策略和优化搜索方法在计算时不依赖于梯度信息或其他辅助知识，而只需要影响搜索方向的目标函数和相应的适应度函数，所以遗传算法提供了一种求解复杂系统问题的通用框架，它不依赖于问题的具体领域，对问题的种类有很强的鲁棒性，所以广泛应用于各种领域。下面是遗传算法的主要应用领域。

1．函数优化

函数优化是遗传算法的经典应用领域，也是对遗传算法进行性能评价的常用算例。很多人构造出了各种各样的复杂形式的测试函数，有连续函数也有离散函数，有凸函数也有凹函数，有低维函数也有高维函数，有确定函数也有随机函数，有单峰值函数也有多峰值函数等。用这些几何特性各具特色的函数来评价遗传算法的性能，更能反映算法的本质效果。而对于一些非线性、多模型、多目标的函数优化问题来说，用其他优化方法较难求解，而用遗传算法都可以方便地得到较好的结果。

2．组合优化

随着问题规模的扩大，组合优化问题的搜索空间也急剧扩大，有时在目前的计算机上用枚举法很难或甚至不可能求出其精确最优解，而遗传算法却能寻求到满意解。实践证明，遗传算法对于解决组合优化中的NP 完全问题非常有效。例如，遗传算法已经在求解旅行商问题、背包问题、装箱问题、图形划分问题等方面得到了成功的应用。

3．生产调度问题

生产调度问题在很多情况下所建立起来的数学模型难以精确求解，即使经过一些简化之

后可以进行求解，也会因简化得太多而使得求解结果与实际相差甚远。而目前在现实生产中主要是靠经验来进行调度的。现在遗传算法已成为解决复杂调度问题的有效工具，在单件生产车间调度、流水线生产车间调度、生产规划、任务分配等方面都得到了有效的应用。

4．自动控制

在自动控制领域中有很多与优化相关的问题需要求解，遗传算法已在其中得到了初步的应用，并显示出了良好的效果。例如，用遗传算法进行航空控制系统的优化、使用遗传算法设计空间交会控制器、基于遗传算法的模糊控制器的优化设计、基于遗传算法的参数辨识、基于遗传算法的模糊控制规则的学习等，都显示出了遗传算法在这些领域中应用的可能性。

5．机器人学

机器人是一类复杂的难以精确建模的人工系统，而遗传算法的起源就来自于对人工自适应系统的研究，所以机器人学理所当然地成为遗传算法的一个重要应用领域。例如，遗传算法已经在移动机器人路径规划、关节机器人运动轨迹规划、机器人逆运动学求解、细胞机器人的结构优化和行为协调等方面得到了研究和应用。

6．图像处理

图像处理是计算机视觉中的一个重要研究领域。在图像处理过程中，如扫描、特征提取、图像分割等不可避免地会存在一些误差，这些误差会影响图像处理的效果。如何使这些误差最小是使计算机视觉达到实用化的重要要求。遗传算法在这些图像处理中的优化计算方面找到了用武之地，目前已在模式识别、图像恢复、图像边缘特征提取等方面得到了应用。

7．人工生命

人工生命是用计算机、机械等人工媒体模拟或构造出的具有自然生物系统特有行为的人造系统。自组织能力和自学习能力是人工生命的两大主要特征。人工生命与遗传算法有着密切的关系，基于遗传算法的进化模型是研究人工生命现象的重要基础理论。虽然人工生命的研究尚处于启蒙阶段，但遗传算法已在其进化模型、学习模型、行为模型、自组织模型等方面显示出了初步的应用能力，并且必将得到更为深入的应用和发展。

8．遗传编程

Koza 发展了遗传编程的概念，使用了以 LISP 语言所表示的编码方法，基于对一种树型结构所进行的遗传操作来自动生成计算机程序。虽然遗传编程的理论尚未成熟，应用也有一些限制，但它已成功地应用于人工智能、机器学习等领域。

9．机器学习

学习能力是高级自适应系统所应具备的能力之一。基于遗传算法的机器学习，特别是分类器系统，在很多领域中都得到了应用。例如，遗传算法被用于学习模糊控制规则，利用遗传算法来学习隶属函数，从而更好地改进模糊系统的性能；基于遗传算法的机器学习可用来调整人工神经网络的连接权，也可用于人工神经网络的网络结构优化设计；分类器系统也在学习多机器人路径规划系统中得到了成功的应用。

5.2 遗传算法的基本流程及实现技术

遗传算法是对自然界中生物遗传与进化机理的模仿。生物染色体用数学方式或计算机方式来体现就是一串数码（位串），即编码。位串中的元素就是基因，表示了不同的特征。针对不同的问题，很多学者设计了许多不同的编码方法来表示问题的可行解，开发出了许多种不同的遗传算子来模仿不同环境下的生物遗传特性。这样，由不同的编码方法和不同的遗传算子就构成了各种不同的遗传算法。但这些遗传算法都有共同的特点，即通过对生物遗传和进化过程中选择、交叉、变异机理的模仿，来完成对问题最优解的自适应搜索过程。基于这个共同特点，Goldberg 总结出了一种统一的最基本的遗传算法——基本遗传算法（Simple Genetic Algorithms，SGA）[14]。基本遗传算法只使用选择算子、交叉算子和变异算子这三种基本遗传算子，其遗传进化操作过程简单，容易理解，是其他一些遗传算法的雏形和基础。它不仅给各种遗传算法提供了一个基本框架，同时也具有一定的应用价值。

下面以基本遗传算法作为主要介绍对象，加上适当的改进，来分析遗传算法的结构和机理。

5.2.1 遗传算法的基本流程

在遗传算法中，通过随机方式产生若干个所求解问题的数字编码，即染色体，形成初始种群；通过适应度函数给每个个体一个数值评价，淘汰低适应度的个体，选择高适应度的个体参加遗传操作，经过遗传操作后的个体集合形成下一代新的种群，再对这个新种群进行下一轮进化。

遗传算法在整个进化过程中的遗传操作是随机性的，但它所呈现出的特性并不是完全随机搜索的，它能有效地利用历史信息来推测下一代期望性能有所提高的寻优点集。这样一代代地不断进化，最后收敛到一个最适应环境的个体上，求得问题的最优解。基本遗传算法的

框图如图 5.1 所示，其中 GEN 是当前代数[15]。

基本遗传算法的主要步骤如下。

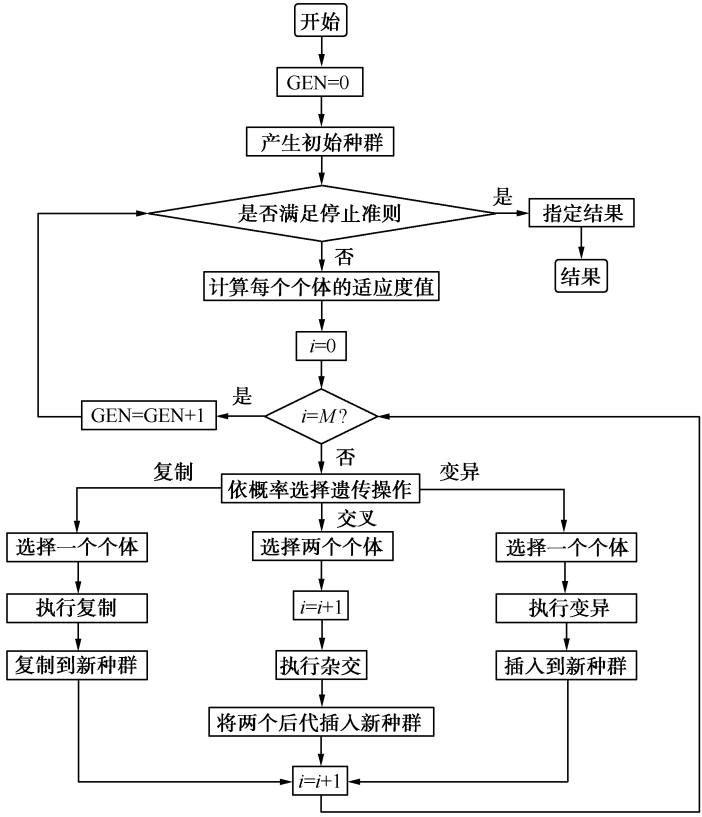


图 5.1　基本遗传算法的框图

（1）随机产生一个由确定长度的特征字符串组成的初始种群。

（2）对该字符串种群迭代地执行下面的步骤①和②，直到满足停止准则为止：

① 计算种群中每个个体字符串的适应度值；

② 应用复制、交叉和变异等遗传算子产生下一代种群。

（3）把在后代中出现的最好的个体字符串指定为遗传算法的执行结果，这个结果可以表示问题的一个解。

5.2.2 遗传算法的实现技术

基本遗传算法由编码、适应度函数、遗传算子（选择、交叉和变异）及运行参数组成。

1．编码

编码是应用遗传算法时要解决的首要问题，也是设计遗传算法时的一个关键步骤。许多应用问题的结构很复杂，但都可以化为简单位串编码来表示。编码方法除决定了个体的染色体排列形式之外，还决定了从搜索空间变换到解空间的解码方法，同时也影响到交叉算子、变异算子等遗传算子的运算方法。由此可见，编码方法在很大程度上决定了如何进行群体的遗传进化运算及遗传进化运算的效率。

由于遗传算法应用的广泛性，人们已经提出了许多种不同的编码方法。最常用的是二进制编码方法。

二进制编码方法将问题空间的参数表示为基于字符集{0，1}构成的符号串。二进制编码符号串的长度与问题所要求的求解精度有关。假设某一个参数的取值范围是$[u,v]$，用长度为 l 的二进制编码符号串来表示该参数，将$[u,v]$等分成 2^l-1 个子部分，每一个等分的长度为δ，则它总共能够产生 2^l 种不同的编码，参数编码的对应关系如下。

$$\begin{array}{ccccc} 00000000 & \cdots & 00000000 & \rightarrow & u \\ 00000000 & \cdots & 00000001 & \rightarrow & u+\delta \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 11111111 & \cdots & 11111111 & \rightarrow & v \end{array}$$

其中，

$$\delta = \frac{v-u}{2^l-1} \tag{5.1}$$

假设某一个体的编码是：

$$X : x_l x_{l-1} x_{l-2} \cdots x_2 x_1 \tag{5.2}$$

则上述二进制编码所对应的解码公式为：

$$x = u + \frac{v-u}{2^l-1} \bullet \sum_{i=1}^{l} x_i 2^{i-1} \tag{5.3}$$

二进制编码方法具有编码、解码操作简单易行，交叉、变异等遗传操作便于实现等优点。但是二进制编码的最大缺点是长度较大，对很多问题来说用其他编码方法可能更有利。其他的编码方法主要有：格雷码编码方法、浮点数编码方法、符号编码方法、多参数编码方法等。

格雷码指的是连续的两个整数所对应的编码值之间只有一个码位是不相同的，其余码位完全相同。例如，十进制数 5 和 6 的二进制编码分别为 0101 和 0110，而格雷码分别为 0111 和 0101。

格雷码有一个特点，即任意两个整数的差是这两个整数所对应的格雷码之间的海明距离（Hamming Distance）。这个特点是遗传算法中使用格雷码进行个体编码的主要原因。

浮点数编码方法是指个体的每个基因值用某一范围内的一个浮点数来表示，个体的编码长度等于其决策变量的个数。因为这种编码方法使用的是决策变量的真实值，所以浮点数编码方法也叫做真值编码方法。

符号编码方法是指个体染色体编码串中的基因值取自一个无数值含义，而只有代码含义的符号集。这个符号集可以是一个字母表，也可以是一个数字序号表，还可以是一个代码表等。

对于旅行商问题来说，采用符号编码方法，按一条回路中城市的次序进行编码。例如，编码串为 154387692 表示从城市 1 开始，依次是城市 5、4、3、8、7、6、9、2，最后回到城市 1。

总的说来，不同的编码方式具有不同的优缺点，有不同的适用范围。目前还不存在一套完整的理论可用以指导选择各类编码。目前在使用何种编码上存在两种观点：一种根据模式定理，建议尽量用少的符号进行编码；另一种以数值优化计算的方便和精度为准，采用一个基因一个参数的方法，并把相应的基因操作改造成适合实数操作的形式。近年来，许多学者发现在有些问题上，采用大符号集编码的遗传算法比采用二进制编码的遗传算法的性能要好。

2．适应度函数

遗传算法将问题空间表示为染色体位串空间，为了执行适者生存的原则，必须对个体位串的适应性进行评价。因此，适应度函数就构成了个体的生存环境。根据个体的适应度值，就可以决定它在此环境下的生存能力。一般来说，好的染色体位串结构具有比较高的适应度函数值，即可以获得较高的评价，具有较强的生存能力。

适应度函数要有效地反映每一个染色体与问题的最优解染色体之间的差距。若一个染色体与问题的最优解染色体之间的差距较小，则对应的适应度函数值之差就较小，否则就较大。适应度函数的取值大小与求解问题对象有很大的关系。

3．选择算子

模仿生物进化的过程，遗传算法使用选择算子来对群体中的个体进行优胜劣汰操作：适应度高的个体被遗传到下一代群体中的概率较大；适应度较低的个体被遗传到下一代群体中的概率较小。遗传算法中的选择操作就是用来确定如何从父代群体中按某种方法选取哪些个体遗传到下一代群体中的一种遗传运算。最常用的选择算子的操作方法是基本遗传算法中的

比例选择算法。

比例选择算法是一种回放式随机采样的方法。它采用赌轮选择机制，令 $\sum f_i$ 表示群体的适应度值的总和，f_i 表示群体中第 i 个染色体的适应度值，它产生后代的能力正好为其适应度值所占份额 $f_i / \sum f_i$ 。

另外，还有以下几种选择算子的操作方法。

最优保存策略指的是当前群体中适应度最高的个体不参与交叉运算和变异运算，而是用它来替换本代群体中交叉、变异等遗传操作后所产生的适应度最低的个体。最优保存策略可视为选择操作的一部分。该策略的实施可保证迄今为止所得到的最优个体不会被交叉、变异等遗传运算所破坏，它是遗传算法具有收敛性的一个保证条件。但另一方面，它也容易使得某个局部最优个体不易被淘汰掉反而快速扩散，从而使得算法的全局搜索能力不强。所以该方法一般要与其他一些选择操作配合使用。

确定式采样选择方法的基本思想是按照一种确定的方式来进行选择操作的。这种选择操作方法可保证适应度较大的一些个体一定能够被保留在下一代群体中，并且操作也比较简单。

无回放选择操作方法也叫做期望值选择方法，它是根据每个个体在下一代群体中的生存期望值来进行选择运算的。这种选择操作方法能够降低一些选择误差，但操作不太方便。

以上的选择操作方法，都是根据各个个体适应度的具体数值进行选择的，一般要求适应度取非负值，这就使得在选择操作之前必须先对负的适应度进行变换处理。而排序选择方法则只根据个体适应度之间的大小关系，对个体适应度是否取正值或负值，以及个体适应度之间的数值差异程度并无特别要求。排序选择方法中各个个体被选中的概率由个体适应度大小排序关系决定。

随机联赛选择也是一种基于个体适应度大小关系的选择方法。该方法每次选取几个个体中适应度最高的一个个体遗传到下一代群体中。在联赛选择操作中，只有个体适应度之间的大小比较运算，而无个体适应度之间的算术运算，所以它对于个体适应度是取正值还是取负值无特别要求。

4．交叉算子

模仿生物遗传进化过程中的胶片重组环节，在遗传算法中使用交叉算子来产生新的个体。遗传算法中的交叉运算，是指对两个相互配对的染色体按某种方式相互交换其部分基因，从而形成两个新的个体。交叉运算是遗传算法区别于其他进化算法的重要特征，它在遗传算法中起着关键作用，是产生新个体的主要方法。

遗传算法中，在交叉运算之前还必须先对群体中的个体进行配对。目前常用的配对策略

是随机配对，即将群体中的 M 个个体以随机的方式组成[M/2]对配对个体组，交叉操作是在这些配对个体组中的两个个体之间进行的。

交叉算子的设计和实现与所研究的问题密切相关，一般要求它既不要太多地破坏个体编码串中表示优良性状的优良模式，又要能够有效地产生出一些较好的新个体模式。另外，交叉算子的设计要和个体编码设计统一考虑。下面简单地介绍几种交叉算子。

单点交叉又称为简单交叉，它是指在个体编码串中只随机设置一个交叉点，然后在该点相互交换两个配对个体的部分染色体。单点交叉的重要特点是：若邻接基因座之间的关系能提供较好的个体性状和较高的个体适应度，则这种单点交叉操作破坏这种个体性状和降低个体适应度的可能性最小。假如有如下 10 位长度的两个个体 P_1 和 P_2。

P_1：1 0 0 0 1 0 1 1 1 0

P_2：1 0 0 1 1 1 0 0 1 1

产生一个在 0～9 之间的随机数，假设现在产生的是 4，将 P_1 和 P_2 的低四位交换：P_1 的高六位与 P_2 的低四位组成数串 1000100011，这就是 P_1 和 P_2 的一个后代个体；P_2 的高六位和 P_1 的低四位组成数串 1001111110，这就是 P_1 和 P_2 的另一个后代个体。

双点交叉是指在个体编码串中随机设置两个交叉点，然后再进行部分基因交换。通过把单点交叉和双点交叉进行推广，就可以形成多点交叉。但是，一般不太使用多点交叉算子，因为它有可能破坏一些好的模式。事实上，随着交叉点数的增多，个体的结构被破坏的可能性也逐渐增大，这样就很难有效地保存较好的模式，从而影响遗传算法的性能。

均匀交叉是指两个配对个体的每一个基因座上的基因都以相同的交叉概率进行交换，从而形成两个新的个体。均匀交叉实际上可归属于多点交叉的范围，其具体运算可通过设置一个屏蔽字来确定新个体的各个基因如何由哪个父代个体来提供。

算术交叉是指由两个个体的线性组合而产生出两个新的个体。为了能够进行线性组合运算，算术交叉的操作对象一般是由浮点数编码所表示的个体。

5．变异算子

模仿生物遗传进化中的变异环节，在遗传算法中引入变异算子来产生新的个体。遗传算法中的变异运算，是指将个体染色体编码串中的某些基因座上的基因值用该基因座的其他等位基因来替换，从而形成一个新的个体。例如，对于二进制编码的个体，其编码字符集为{0，1}，变异操作就是将个体在变异点上的基因值取反，即用 0 替换 1，或用 1 替换 0；对于浮点数编码的个体，若某一变异点处的基因值的取位范围为[A,B]，变异操作就是用该范围内的一个随机数去替换原基因值；对于符号编码的个体，若其编码字符集为{A,B,C,…}，变异操作就是用这个字符集中的一个随机指定的且与原基因值不相同的符号去替换变异点上的原有符号。

例如，有如下的 8 位二进制编码：

1 0 1 0 0 1 1 0

随机产生一个 1～8 之间的数 k，假如现在 k=5，对从右往左的第 5 位进行变异操作，将原来的 0 变为 1，得到如下数据串：

1 0 1 1 0 1 1 0

对遗传运算过程中产生新个体的能力方面来说，交叉运算是产生新个体的主要方法，它决定了遗传算法的全局搜索能力；而变异运算只是产生新个体的辅助方法，但它也是必不可少的一个运算步骤，因为它决定了遗传算法的局部搜索能力。交叉算子与变异算子的相互配合，共同完成了对搜索空间的全局搜索和局部搜索，从而使得遗传算法能够以良好的搜索性能完成最优化问题的寻优过程。

6．运行参数

遗传算法的运行依赖各种各样的参数。这些参数主要包括编码长度 L，种群规模 N，交叉概率 P_c，变异概率 P_m，终止进化代数 T，这些参数对于遗传的运行性能有重要的影响。

（1）编码长度 L：编码长度 L 的选择取决于特定问题解的精度。要求的精度越高，编码长度越长。使用二进制编码时，L 通常由问题的求解精度 ε 决定；使用实数编码时，L=n 与问题的自变量维数相等；使用符号编码时，L 由对问题的编码方式来确定；另外，也可以使用变长度的编码来表示个体。

（2）种群规模 N：种群规模 N 表示每一代种群中所含个体数目。当 N 取值较小时，可提高遗传算法的运算速度，但却降低了种群的多样性，容易引起遗传算法早熟。但种群数目较大时，将增加个体适应性评价的计算量，从而使收敛速度降低。一般情况下专家建议 N =20～200。

（3）交叉概率 P_c：交叉概率控制着交叉算子的应用频率。在每一代新的群体中，需要对 $P_c \times n$ 个个体的染色体结构进行交叉操作。一般来说，较大的 P_c 容易破坏种群中已形成的优良模式，使搜索具有太大随机性，而较小的 P_c 使发现新个体的速度太慢。一般建议的取值范围是 0.4～0.99。

（4）变异概率 P_m：变异操作是保持群体多样性的有效手段。变异概率太小，则变异操作产生新个体的能力和抑制早熟现象的能力就会较差；而变异概率过高，则遗传搜索将变成随机搜索。一般取 P_m =0.005～0.01。

（5）终止进化代数 T：终止代数 T 是遗传算法运行结束条件的一个参数，它表示遗传算法运行到指定的进化代数之后就停止运行，并将当前群体中的最佳个体作为所求问题的最优解输出。一般取 100～1000。

到目前为止，对于遗传算法进化参数的设置还没有成熟的原则和方法，基本上依赖经验和对所求解问题的了解。

5.3　遗传算法的基本原理[13,15,16]

遗传算法的基本原理主要涉及以下两个方面：第一，有关遗传算法的搜索机理，即回答遗传算法是如何工作的。第二，有关算法的性态分析。例如，所给定的一个遗传算法执行策略是收敛的吗？它是进化到某个局部最优还是全局最优？如果一个遗传算法是收敛的，它需要多长时间收敛？模式定理和基因块假设是人们早期对遗传算法搜索机理的说明。收敛性理论能够回答第二个方面的问题。

5.3.1　模式定理

定义 5.1　扩展位串空间 $S_e^L=\{0,1,*\}^L$ 上的一个模式 H 可以表示为：

$$H=\{a\mid a\in S^L,\forall i,H_i\neq *\Rightarrow H_i=a_i\} \tag{5.4}$$

其中，$a=(a_1,a_2,\cdots,a_L),H=(H_1,H_2,\cdots,H_L),a_i\in\{0,1\},H_i\in\{0,1,*\},i=1,2,\cdots,L;a\in S^L$，$H\in S_e^L$。

根据模式的定义，以二进制编码方式为例，个体是由二值字符集{0，1}中的元素所组成的一个编码串，而模式却是由三值字符集{0，1，*}中的元素组成的一个编码串，其中“*”表示通配符，它既可被当做“1”，也可被当做“0”。

例如，模式 H =10**1 描述了长度为 5，且在位置 1，5 取值为“1”，在位置 2 取值为“0”的所有字符串的集合{10001，10011，10101，10111}；模式 H ={11100}所描述的个体集合是由它自身组成的，即{11100}。由这些例子可以看出，模式的概念使得我们可以简明地描述具有相似结构特点的个体编码字符串。

在引入模式概念之后，遗传算法的本质是对模式所进行的一系列运算，即通过选择算子将当前群体中的优良模式遗传到下一代群体中，通过交叉算子进行模式的重组，通过变异算子进行模式的突变。通过这些遗传运算，一些较差的模式逐步被淘汰，而一些较好的模式逐步被遗传和进化，最终就可以得到问题的最优解。

定义 5.2　模式的阶（schema order）是指模式中所含有 0，1 确定基因位的个数，记做 $O(H)$。

对于二进制编码字符串而言，模式的阶就是模式中所含有的 1 和 0 的数目。例如，$O(11*0**0)=4$，$O(1*******)=1$。当字符串的长度固定时，模式阶数越高，能与该模式匹配的字符串（称为样本）数就越少，因而该模式的确定性也就越高。

定义 5.3　模式的定义长度（schema dimension）是指模式中从左到右第一个非*位和最后一个非*位之间的距离，记做 $\delta(H)$。

例如，$\delta(10***1**)=5$，$\delta(**0**1)=3$。而对于 H =*****1，H =1*****，H =***1* 之类的模式，由于它们只有一位确定的基因值，这个位置既是第一个确定基因值位置，也是最后一个确定基因值位置，所以规定它们的模式定义长度为 1，即 $\delta(***1**)=1$。

定义 5.4 令 $m=m(H,t)$ 为模式 H 在第 t 代群体中所含位串数量，模式在第 t 代群体中包含的个体位串为 $\{a_1,a_2,\cdots,a_m\}$，称为模式 H 在群体中的生存数量或采样样本，$a_j\in H(j=1,2,\cdots,m)$，则模式 H 在第 t 代群体中的适应度值估计为：

$$f(H,t)=\sum_{j=1}^{m} f(a_j)\Big/m \tag{5.5}$$

即模式的适应度值估计（简称模式的适应度值）是群体中所包含的全部个体的适应度值的平均值。

在引入模式概念之后，遗传算法在群体进化过程中，可以看做是通过选择、交叉和变异算子，不断发现重要基因、寻找较好模式的过程。高适应度值的个体被选择概率大于低适应度值的个体，同样根据模式适应度值的定义，选择算子对于模式的作用表现为其适应度值越高被选择的概率也就越大。所以，好的模式在群体中的个体采用数量会不断增加，其上的重要基因或有效基因也得以遗传下来。对交叉算子来说，如果它不分割一个模式的话，则该模式不变，反之可以导致模式消失或所包含的高适应度值个体数量减少，同时交叉算子还可以创建新的模式。变异算子的变异率很小，对模式生成和破坏的概率也很小。

下面具体分析基本遗传算法中选择算子、交叉算子和变异算子对模式 H 的生存数量的影响。假设 $P(t)$ 为第 t 代规模为 n 的群体，$P(t)=\{a_1(t),a_2(t),\cdots,a_n(t)\}$。

1．选择算子对模式 H 的生存数量的影响

假定在 t 代群体 $P(t)$ 中模式 H 的生存数量为 $m(H,t)$，在选择操作过程中个体按概率 $p_i=f(a_i)/\sum_{i=1}^{n} f(a_i)$ 被选择（$f(a_i)$ 为个体的适应度函数），则在 $t+1$ 代群体，模式 H 的生存数量为：

$$m(H,t+1)=m(H,t)\times n\times f(H,t)/\sum_{i=1}^{n} f(a_i) \tag{5.6}$$

将群体的平均适应度值表示为 $\overline{f}=\sum_{i=1}^{n} f(a_i)/n$，所以上式可表示为：

$$m(H,t+1)=m(H,t)\times(f(H,t)/\overline{f}) \tag{5.7}$$

该式说明下一代群体中模式 H 的生存数量与模式的适应度值成正比，与群体平均适应度值成反比。当 $f(H,t)>\overline{f}$ 时，H 的生存数量增加；当 $f(H,t)<\overline{f}$ 时，H 的生存数量减少。群体中任一模式的生存数量都将在选择操作中按上面的规律变化。

2．交叉算子对模式 H 的生存数量的影响

交叉操作对模式的影响与其定义长度 $\delta(H)$ 有关。$\delta(H)$ 越大，模式被破坏的可能性越大。若染色体位串长度为 L，在单点交叉算子作用下模式 H 的存活概率 $p_{\text{survival}}=1-\delta(H)/(L-1)$。在交叉概率为 p_c 的单点交叉算子作用下，该模式的存活概率为：

$$p_{\text{survival}} \geqslant 1-p_c\times\delta(H)/(L-1) \tag{5.8}$$

那么，模式 H 在选择、交叉算子共同作用下的生存数量可用下式计算：

$$\begin{aligned} m(H,t+1) &\geqslant m(H,t)\times(f(H,t)/\overline{f})\times p_{\text{survival}} \\ &= m(H,t)\times(f(H,t)/\overline{f})\times(1-p_c\times\delta(H)/(L-1)) \end{aligned} \tag{5.9}$$

可见，在选择、交叉算子共同作用下，模式生存数量的变化与其平均适应度值及定义长度 $\delta(H)$ 密切相关。当 $f(H,t)>\overline{f}$，且 $\delta(H)$ 较小时，群体中该模式生存数量以指数规律增长；反之则以指数规律减少。

3．变异算子对模式 H 的生存数量的影响

对应群体中的任一个体，变异操作就是以概率 p_m 随机改变某一基因位的等位基因。为了使模式 H 在变异操作中生存下来，其上所有确定位的等位基因均不发生变化的概率为 $(1-p_m)^{O(H)}$。一般情况下 p_m <<1，所以模式 H 的生存概率可近似表示为 $(1-p_m)^{O(H)}=1-p_m\times O(H)$。

通过三个遗传算子对模式的生存数量影响的分析，可以得到如下结论。

定义 5.5　在选择、交叉、变异遗传算子的作用下，那些低阶、定义长度短、超过群体平均适应度值的模式的生存数量，将随着迭代次数的增加以指数规律增长。

这就是模式定理，称为遗传算法进化动力学的基本定理。该定理反映了重要基因的发现过程。重要基因对应于较高的适应度值，说明了它们所代表的个体在下一代有较高的生存能力，是提高群体适应性的进化方向。

5.3.2　积木块假设

模式定理说明了具有某种结构特征的模式在遗传进化过程中其样本数将按指数级增长，这种模式就是具有低阶、定义长度短，且平均适应度值高于群体平均适应度值的模式。这种类型的模式被称为基因块或积木块。

之所以称为基因块，是由于遗传算法的求解过程并不是在搜索空间中逐一地测试各个基因的枚举组合，而是通过一些较好的模式，像搭积木一样，将它们拼接在一起，从而逐渐地构造出适应度越来越高的个体编码串。模式定理不仅仅说明了基因块的样本呈指数级增长，也说明了用遗传算法寻求最优样本的可能性，但它并未指明遗传算法一定能够寻求到最优解，而积木块假设却说明了遗传算法的这种能力。

积木块假设：个体的基因块通过选择、交叉、变异等遗传算子的作用，能够相互拼接在一起，形成适应度更高的个体编码串。

积木块假设说明了用遗传算法求解各类问题的基本思想，即通过积木块直接相互拼接能够产生出更好的解。基于模式定理和积木块假设，就使得我们能够在很多应用问题中广泛地使用遗传算法的思想。需要说明的是，虽然积木块假设并未得到完整而严密的数学证明，但大量的应用实践说明了其有效性。但也有反例（即所谓的遗传算法欺骗问题）说明这一假设的不真实性。

5.3.3 收敛性理论

对于优化问题求解的任何搜索算法而言，其收敛性具有重要的理论意义。因此，遗传算法的收敛性一直是理论研究的一个主要方面。但是，遗传算法的全局优化收敛性的理论分析尚未完全解决，基本遗传算法并不保证全局最优收敛，而只能在一定的约束条件下，实现全局最优收敛。

1．遗传算法收敛性的定义

遗传算法是一种随机搜索算法，可以从不同的角度定义它的收敛性。

1）渐近收敛

与其他一些随机搜索算法（如模拟退火算法）的不同之处在于，遗传算法维持了一个具有一定数目个体的种群。所以，在定义算法收敛性时就存在两种思路：一种是针对整个种群进行定义，另一种是针对个体进行定义。米哈莱威兹（Michalewicz）[17,18]给出了针对整个种群的一种渐进收敛性的定义，将所有可能的种群所组成的集合视为一个状态空间 X，算法在 t 时刻的种群为 x_t。于是，可对算法的收敛性定义如下。

定义 5.6 若算法在 t 时刻的种群满足：

$$\lim_{t\to\infty} x_t = x_0, \qquad x_0 \in X \tag{5.10}$$

则称算法收敛到 x_0。

2）概率收敛

由于遗传算法具有随机性，而且在利用遗传算法求解问题时，往往并不知道适应度函数的最大值究竟是多少。所以，当最优个体出现时，算法仍有可能继续进行。但是在实际应用中，总是希望算法收敛时能够得到最优解。因此，在定义其收敛性时应当考查在随机因素作用下算法收敛到最优解的能力。鲁道夫（Rudolph ）[19]给出了一种针对个体收敛性的定义。

定义 5.7　设 Z_t 为 t 时刻种群中所包含的个体的适应度的最大值，f^* 为适应度函数 $f(x)$ 在所有可能的个体所组成的集合 X 中所取的最大值。若 Z_t 满足：

$$\lim_{t\to\infty} P\{Z_t = f^*\} = 1 \tag{5.11}$$

则称算法收敛到最优解。

鲁道夫通过马尔可夫链方法证明，在这个定义下，经典遗传算法不会收敛到最优解。但是若在遗传算法中保留每一代的最优个体，则算法将收敛到最优解。

2．基于马尔可夫链的收敛性分析

遗传算法是不断进行重复选择、交叉与变异的过程，每一种遗传操作都仅与当前状态有关，而与以前的状态无关。因此遗传算法可描述为马尔可夫链（Markovchain），从而其收敛性可应用马尔可夫链理论加以研究。

1）马尔可夫链的定义及相关性质

定义 5.8　（马氏链）设 $\{\hat{X}_n; n \geqslant 0\}$ 为一列取值在离散集的随机变量，离散值的全体（即离散集）记为 $H_L = \{j\}$，称 H_L 为状态空间。若对任意 $n \geqslant 1, i_k \in H_L (k \leqslant n+1)$ 有：

$$P\{\hat{X}_{n+1} = i_n + 1 \mid \hat{X}_n = i_n, \cdots, \hat{X}_0 = i_0\} = P\{\hat{X}_{n+1} = i_n + 1 \mid \hat{X}_n = i_n\} \tag{5.12}$$

则称 $\{\hat{X}_n; n \geqslant 0\}$ 为马氏链（马尔可夫链）。

定义 5.8 是指 $\{\hat{X}_n\}$ 取值的无后效性（即仅与当前状态有关），这种无后效性对于简化条件概率的计算非常重要。

定义 5.9　对任何正整数 m,n，记马氏链 $\{\hat{X}_n\}$ 在 m 时刻处于状态 i 且经过 n 步转移到状态 j 的概率为：

$$P_{ij}(m,n) = P(\hat{X}_{m+n} = j \mid \hat{X} = i\} \tag{5.13}$$

如果上述转移概率与时刻 m 无关，即 $P_{ij}(m,n) \equiv P_{ij}^{(n)}$，则称马氏链 $\{\hat{X}_n\}$ 是齐次的。称 $P_{ij}^{(n)}$ 为马氏链 $\{\hat{X}_n\}$ 的 n 步转移概率。由 $\{\hat{X}_n\}$ 的一步转移概率 $P_{ij}^{(1)}$ 所组成的矩阵 $\boldsymbol{P} = \left[P_{ij}^1\right]$ 称为 $\{\hat{X}_n\}$ 的转移概率矩阵。

2）基本遗传算法的收敛性分析

基本遗传算法可描述为一个齐次马尔可夫链 $P_t=\{P(t),t\geqslant 0\}$，因为基本遗传算法的选择、交叉和变异操作都是独立随机进行的，新群体仅与其父代群体及遗传操作算法有关，而与其父代群体之前的各代群体无关，即群体无后效性，并且各代群体之间的转移概率与时间的起点无关。对于基本遗传算法的收敛性分析，有以下的两个定理。

定理 5.1 基本遗传算法收敛于最优解的概率小于 1。

由定理 5.1 可知，对于这种收敛于最优解的概率小于 1 的基本遗传算法，其应用可靠性就值得怀疑。从理论上来说，仍希望基本遗传算法能够保证收敛于最优解，这就需要对基本遗传算法进行改进，如使用保留最佳个体策略就可达到这个要求。

定理 5.2 使用保留最佳个体策略的遗传算法能收敛于最优解的概率为 1。

定理 5.2 说明了这种使用保留最佳个体策略的遗传算法总能够以概率 1 搜索到最优解。这个结论除了理论上具有重要意义之外，在实际应用中也为最优解的搜索过程提供了一种保证。

3．未成熟收敛

未成熟收敛是遗传算法中不可忽视的现象，它主要表现在以下两个方面：一是群体中所有的个体都陷于同一极值而停止进化；二是接近最优解的个体总是被淘汰，进化过程不收敛。

在遗传算法的处理过程中每个环节都有可能导入产生未成熟收敛的因素，具体表现为：

（1）在进化初始阶段，生成了具有很高适应度的个体 X。

（2）在基于适应度比例的选择下，其他个体被淘汰，大部分个体与 X 一致。

（3）相同的两个个体实行交叉，从而未能生成新个体。

（4）通过变异或逆转所生成的个体适应度高但数量少，所以被淘汰的概率很大。

（5）群体中大部分个体都处于与 X 一致的状态。

针对上述情况，需要在编码、适应度函数和遗传操作等设计中考虑抑制未成熟收敛因素的对策。这些对策包括如下几个方面。

（1）提高变异概率：在进化初始阶段，它可以加强遗传算法的随机搜索能力。

（2）调整选择概率：可以把选择概率本身也作为个体来进行优化，这就是所谓元遗传算法。

（3）合适定标：对适应度函数定标。

（4）维持群体中个体的多样性。为此，需要增加群体规模，但要考虑计算量增大的因素；实施局部化，把群体分割成若干子群体，每个子群体独立地进行选择操作，这样可使因出现不适当个体而产生未成熟收敛的现象局部化；实施单一化，把相同个体单一化，即不允许群体中有若干个相同个体出现；增大配对个体距离，配对选择一般是随机进行的，其中缺少对个体间相似度的判断，因此有可能使交叉结果未能产生新个体。

以上对策的效果各不相同。为了有效地克服未成熟收敛，需要在进化过程中分阶段地交替使用这些对策。

5.4　遗传算法的改进

遗传算法以其基本思想简单、便于实现和并行搜索的优点赢得了众多学者和工程人员的青睐，是目前应用最广的优化搜索算法之一。但遗传算法存在收敛速度慢和易于陷入局部最优的问题，在需要优化的参数较多时，更凸显了遗传算法的不足。如何提高遗传算法跳出局部最优的能力和如何提高遗传算法的收敛速度成为近年来遗传算法的研究热点。许多学者从不同的角度对遗传算法进行了改进，使遗传算法的寻优能力有了不同程度的提高。

5.4.1　混合遗传算法

目前，对遗传算法的研究主要集中在数学基础、各环节的实现方式及与其他算法的结合方面。其中，尤以遗传算法与其他算法相结合方面的研究最引人关注。由于遗传算法具有开放式的结构，与问题的关联性不大，很容易和其他算法进行结合，所以融合了其他的算法思想和遗传算法思想的混合遗传算法成了目前改进遗传算法研究的一个重要方向。混合遗传算法的实现方法体现在两个方面。

（1）引入了局部搜索过程：基于群体中各个个体所对应的表现型，进行局部搜索，从而找到各个个体在目前的环境下所对应的局部最优解，以便达到改善群体总体性能的目的。

（2）增加了编码交换过程：对局部搜索过程所得到的局部最优解，再通过编码过程将它们交换为新的个体，以便能够以一个性能较优的新群体为基础来进行下一代的遗传进化操作。

比较典型的混合遗传算法是模拟退火遗传算法（Simulated Annealing Genetic Algorithm，SAGA）。模拟退火遗传算法的基本思想是通过模拟高温物体退火过程的方法来找到优化问题的全局最优或近似全局最优解。从统计物理学的观点来看，随着温度的降低，物质的能量将逐渐趋近于一个较低的状态，并最终达到某种平衡。遗传算法的局部搜索能力较差，但把握搜索过程总体的能力较强；而模拟退火遗传算法具有较强的局部搜索能力，并能使搜索过程避免陷入局部最优解的问题，但它却对整个搜索空间的了解不多，不便于使搜索过程进入最有希望的搜索区域，从而使得模拟退火遗传算法的运算效率不高。但如果将遗传算法和模拟退火遗传算法相结合，互相取长补短，则有可能开发出性能优良的新的全局搜索算法。目前，已有许多学者将退火机制引入到遗传操作中，使遗传操作产生优良个体的概率增加，并使遗传算法的寻优能力有了明显的提高[20~22]。

与基本遗传算法的总体运行过程相类似，模拟退火遗传算法也是从随机产生的初始解（初始群体）开始全局最优解搜索过程的。它先通过选择、交叉和变异等遗传操作来产生一组新的个体，然后再独立地对所产生出的各个个体进行模拟退火过程，以其结果作为下一代群体中的个体。这个运行过程反复迭代地进行，直到满足某个终止条件为止。

模拟退火遗传算法可描述如下。

（1）进化代数计数器初始化：$t \leftarrow 0$。

（2）随机产生初始群体 $p(t)$。

（3）评价群体 $p(t)$的适应度。

（4）个体交叉操作：$[p'(t)] \leftarrow \text{Crossover}[p(t)]$。

（5）个体变异操作：$[p''(t)] \leftarrow \text{Mutation}[p'(t)]$。

（6）个体模拟退火操作：$p'''(t) \leftarrow \text{SimulatedAnnealing}[p''(t)]$

（7）评价群体 $p'''(t)$ 的适应度。

（8）个体选择、复制操作：$p(t+1) \leftarrow \text{Reproduction}[p(t) \cup p'''(t)]$。

（9）终止条件判断。若不满足终止条件，则 $t \leftarrow t+1$，转到步骤（4），继续进化过程；若满足终止条件，则输出当前最优个体，算法结束。

5.4.2 自适应遗传算法

遗传算法的参数中，交叉概率 p_c 和变异概率 p_m 的选择是影响遗传算法行为和性能的关键所在，直接影响算法的收敛性，p_c 越大，新个体产生的速度就越快。然而，当 p_c 过大时，遗传模式被破坏的可能性也越大，使得具有高适应度的个体结构很快就会被破坏。但是，如果 p_c 过小，会使搜索过程缓慢，以至停滞不前。对于变异概率 p_m，如果 p_m 过小，则不易产生新的个体结构；如果 p_m 取值过大，则遗传算法就变成了纯粹的随机搜索算法。针对不同的优化问题，需要反复试验来确定 p_c 和 p_m，这是一项烦琐的工作，而且很难找到适应于每个问题的最佳值。

Srinivas[23]等人提出了一种自适应遗传算法（Adaptive GA，AGA），使 p_c 和 p_m 能够随着适应度值自动改变。当种群各个个体适应度值趋于一致或趋于局部最优时，使 p_c 和 p_m 增加，而当群体适应度值比较分散时，使 p_c 和 p_m 减少。同时，对于适应度值高于群体平均适应度值的个体，对应于较低的 p_c 和 p_m，使该个体能够被保护进入下一代；而适应度值低于平均适应度值的个体，对应于较高的 p_c 和 p_m，使该个体被淘汰。因此，自适应遗传算法可根据种群的进化情况来动态地调整交叉概率 p_c 和变异概率 p_m，以达到克服过早收敛及加快搜索速度的目的。根据其原理，建立的表达式如下：

$$p_c=\begin{cases}\dfrac{k_1(f_{\max}-f')}{(f_{\max}-f_{\text{avg}})}, & f'\geqslant f_{\text{avg}}\\ k_2, & f'<f_{\text{avg}}\end{cases} \tag{5.14}$$

$$p_m=\begin{cases}\dfrac{k_3(f_{\max}-f)}{(f_{\max}-f_{\text{avg}})}, & f\geqslant f_{\text{avg}}\\ k_4, & f<f_{\text{avg}}\end{cases} \tag{5.15}$$

式中，k_1、k_2、k_3、k_4 为（0,1）区间的常数，具体取值根据实际情况确定；$f_{\max}$ 为当代群体中最大的适应度值；f_{avg} 为当代群体的平均适应度值；f'为两个交叉个体中适应度值较大的一个；f 为变异个体的适应度值。

5.4.3　变长度染色体遗传算法

1989 年，Glodberg 等人提出了 MessyGA（MGA[24]），是一种典型的变长度染色体遗传算法，该算法在不影响模式定义长度的情况下，使优良的模式得以增值。

在生物进化过程中，其染色体的长度并不是固定不变的，而是随着进化过程也在慢慢地变化。另外，在遗传算法的实际应用中，有时为简化描述问题的解，也需要使用不同长度的编码串。例如，用遗传算法对人工神经网络结构进行优化设计时，如果各层的节点数是未知的，则个体的染色体长度可以描述为变化的。该算法的基本思想如下。

1．变长度遗传算法的编码和解码

将常规遗传算法的染色体编码串中各基因位的位置与相应的基因值组成一个二元组，把这个二元组按一定顺序排列起来，就组成了变长度染色体的一种通用染色体编码方式。一般它可表示为：

$$X^m:(i_1,v_1)(i_2,v_2)\cdots(i_k,v_k)\cdots(i_n,v_n) \tag{5.16}$$

上述变长度染色体的描述形式中，i_k 是所描述的基因在原常规染色体中的基因位编号，v_k 为对应的基因值。

2．切断算子和拼接算子

MessyGA 由于编码长度可变，遗传操作算子的选择具有特殊性，一般选择算子选用锦标赛选择方法，不再使用通用的交叉算子，而代之以使用下述的切断算子和拼接算子，以它们作为产生新个体的主要遗传算子。

切断算子以某一预先指定的概率，在变长度染色体中随机选择一个基因位，在该处将个体的基因型切断，使之成为两个个体的基因型。

拼接算子以某一预先指定的概率，将两个个体的基因型连接在一起使它们合并为一个个体的基因型。

3．变长度染色体遗传算法的基本结构

变长度染色体遗传算法的结构可描述如下。

（1）初始化：随机产生 M 个长度全部为 k 的染色体，以它们作为变长度染色体遗传算法的初始个体集合 pop(0)，其中 k 为根据问题的不同而设定的一个参数。

（2）适应度评价：对变长度的染色体进行解码、评价和计算各个个体的适应度。

（3）基本处理阶段：对群体 pop(t)施加选择算子，以保留适应度较高的个体。

（4）并列处理阶段：对群体 pop(t)施加变异算子、切断算子和拼接算子，以生成新的个体。

（5）重复步骤（2）到（4），直到满足终止条件为止。

5.4.4 小生境遗传算法

在生物学中，小生境（Niche）是指特定环境下的一种组织功能。在自然界中，生物在其进化过程中，一般总是与自己特征、性状相似的物种生活在一起，共同繁衍后代；它们也都在某一特定的地理区域中生存。在这些群体内部，也不失有一些优秀个体。

作为遗传算法模拟对象的生物都有其特定的生存环境，那么借鉴此概念，可以让遗传算法中的个体在一个特定的生存环境中进化，即在遗传算法中引进小生境技术，将每一代个体划分为若干类，在每个类中选出若干适应度较大的个体作为一个类的优秀代表组成一个种群，再在不同种群之间通过交叉、变异产生新一代个体群，同时采用预选择机制、排挤机制或共享机制完成选择操作。这种基于小生境技术的遗传算法（Niched Genetic Algorithms，NGA），可以更好地保持解的多样性，同时具有很高的全局寻优能力和收敛速度。

遗传算法中模拟小生境的方法主要建立在对常规选择操作的改进基础之上，主要有以下几种。

1．基于预选择的小生境实现方法

Cavicchio[25,26]在 1970 年提出了基于预选择机制的小生境实现方法，其基本思想是：当新产生的子代个体的适应度超过其父代个体的适应度时，所产生出的子代个体才能替换其父代个体而遗传到下一代群体中，否则父代个体仍保留在下一代群体中。由于子代个体和父代个体之间编码结构的相似性，所以这种编码方法替换掉的只是一些编码结构相似的个体，故它能够有效地维持群体的多样性，并造就小生境的进化环境。

2．基于排挤的小生境实现方法

De Jong[5]在 1975 年提出了基于排挤机制的选择策略，其基本思想是：设置一个排挤因子 CF，由群体中随机选择的 1/CF 个个体组成排挤成员，然后依据新产生的个体与排挤成员的相似性来排挤掉一些与排挤成员相似的个体。这里，个体之间的相似性可用个体编码串之间的海明距离来度量。随着排挤过程的进行，群体中的个体逐渐被分类，从而形成各个小的生存环境，并维持了群体的多样性。

3．基于共享函数的小生境实现方法

Goldberg[27]等人在 1987 年提出了基于共享机制的选择策略，其基本思想是：通过反映个体之间相似程度的共享函数来调整群体中各个个体的适应度，从而在这以后的群体进化过程中，算法能够依据这个调整后的新的适应度进行选择运算，以维护群体的多样性，创造出小生境的进化环境。

5.4.5　并行遗传算法

伴随着遗传算法应用的深入开展，并行遗传算法[28]（Parallel Genetic Algorithms，PGA）及其实现过程的研究也变得十分重要。一般来说，遗传算法中适应度的计算最费时间，再加上需要不断地产生新一代，而每一代又有若干个个体，所以如何提高遗传算法的运行速度显得尤为突出。由于遗传算法的内在并行机制，其并行处理是很自然的解决途径。

在并行遗传算法中，引入了一个新的算法——迁移（Migration），它是指在进化过程中子群体间交换个体的过程。一般的迁移方法是将子群体中最好的个体发给其他的子群体，通过迁移可以加快较好个体在群体中的传播，提高收敛速度和解的精度。与单种群相比只需要较少的个体评价计算工作量，即使是采用单一处理器的计算机上以串行方式（伪并行）实现并行算法也能产生较好的结果。因此，采用迁移算子，可使并行算法更适合于全局寻优，并且计算量较小。

遗传算法都有一定的性能评价指标，对于并行遗传算法，人们也提出了许多不同的评价指标，其中最重要的一个评价标准是加速比。设 T_1 为某算法在串行计算机上的运行时间，T_p 是该算法在有 p 个处理器所构成的并行机上的运行时间，则此算法在该并行机上的加速比 S_p 定义为：$S_p=T_1/T_p$。

但对于并行遗传算法来说，由于搜索的随机性，仅使用加速比这个指标来衡量其性能的优劣程度是比较困难的。因此，需要设计出一些具有不同几何特性的测试函数，通过它们来测量和统计达到最优点时的平均进化代数和平均计算时间，根据这些测试结果来比较不同的

并行遗传算法的优劣程度。并行遗传算法的性能主要体现在收敛速度和精度两个方面，它们除了与迁移策略有关，还与一些参数选取的合理性密切相关，如遗传代数、群体数目、群体规模、迁移率和迁移间隔。

1）遗传代数和群体规模

目前大多数研究者采用固定的遗传代数作为算法终止条件，遗传代数越大，求解精度越高，但时间开销越大。如何针对一个具体问题确定一个合理的遗传代数，仍没有一个很好的办法。群体规模是群体个体的数目，群体规模增大有利于解的精度和群体多样性的提高，但同时也增加了求解的时间。

2）迁移率和迁移间隔

将每次被迁移的个体数目称为迁移率。迁移率的选取是一个很复杂的问题：由于被迁移者一般均是各子群体中的最优个体，所以迁移率较大，则有利于优良个体在整个群体中的传播速度和收敛速度的提高，但同时也会增大通信的开销，使加速比下降，也可能导致群体多样性的下降，不利于开发并行遗传算法在多个方向同时进行搜索的特征。应该针对具体问题选取合适的迁移率。

迁移间隔是指相邻两次迁移的时间间隔。迁移间隔小有利于子群体之间的融合，使得优良个体及时传播到所有子群体中，对群体的进化方向可以起到良好的指导作用，有利于提高解的精度和群体的收敛速度。但同时也会明显地增大通信及同步开销，不利于加速比的提高，而且某些优良个体在群体中的统治地位会产生不利于群体保持多样性的负面影响，使得整个群体类似于串行算法中的随机交配群体，不利于并行遗传算法发挥其并发搜索多个方向的特性，并有可能使群体进化陷入局部最小点。如果迁移间隔较大，则各子群体之间比较隔绝，其优点是降低了通信开销，提高了加速比，但同时会导致优良个体不能被及时传播，不能充分发挥其导向作用，不利于提高解的精度和收敛速度。

总之，如何获得较好的性能是并行遗传算法中的重要课题。选取合理的参数是十分困难的，这方面目前还没有指导性的实验结论。

目前并行遗传算法的实现方案大致可分为三类。

1）全局型——主从式模型（Master-Slave Model）

它是串行遗传算法的一种直接并行化方案，在计算机上以 Master-Slave 编程模式实现。它只有一个种群，所有个体的适应度都根据整个种群的适应度计算，个体之间可以任意匹配，每个个体都有机会和其他个体杂交并竞争，因而在种群上所做的选择和匹配是全局的。对于这个模型有多种实现方法：第一种方法是仅仅对适应度函数计算进行并行处理；第二种方法是对遗传算子进行并行处理。全局模型易于实现，计算时间主要用在评价上，这是一种非常有效的并行化方法。

它最大的优点是简单，保留了串行 GA 的搜索行为，因而可直接应用 GA 的理论来预测

一个具体问题能否映射到并行 GA 上求解。当适应度估值操作比其他遗传算子计算量大得多时，它是很有效的，并且不需要专门的计算机系统结构。

2）独立型——粗粒度模型（Coarse-grained Model）

将种群分成若干个子群并分配给各自对应的处理器，每个处理器不仅独立计算适应度，而且独立进行选择、交叉和变异操作，还要定期地相互传送适应度最好的个体，从而加快满足终止条件的要求。粗粒度模型也称为孤岛模型（Island Model），基于粗粒度模型的遗传算法也称为分布式遗传算法（Distributed Genetic Algorithm，DGA）,它是目前应用最广泛的一种并行遗传算法。

Pettey[29]等人已证明，综合考虑选择、交叉和变异的效应，粗粒度模型对遗传模式积木块的搜索次数的上限可用指数函数来描述，这一结果从理论上表明该模型是有效的。粗粒度模型对并行系统平台要求不高，可以是松散耦合并行系统，特别适合基于 Transputer 的 MIMD 系统，并且效果很好，它主要开发群体之间的并行性。

3）分散型——细粒度模型（Fine-grained Model）

为种群中的每一个个体分配一个处理器，每个处理器进行适应度的计算，而选择、交叉和变异的操作仅在与之相邻的一个处理器之间互相传递的个体中进行。

细粒度模型也称为邻域模型（Neighborhood Model）、元胞模型（Cellular Model），适合于连接机、阵列机和 SIMD 系统。

这种算法将遗传算法与元胞自动机相结合。首先将每一个染色体放到每一个处理器或元胞上。在这种模型当中，为了方便实现，节省通信开销，每个染色体（也就是处理器）只和与它相邻的染色体（即处理器）进行通信。每个处理器在它的邻居当中找到一个最好的个体（或依照一定概率）进行交叉。在这里每次交叉操作只产生一个子代，然后这个新产生的子代就代替原来在这个处理器上的个体而占据这个处理器。这种算法的主要思想是将交叉操作、选择操作局限在一个很小邻居的范围内。

5.5　小结

遗传算法是进化计算的一个部分，是模拟达尔文的遗传选择和自然淘汰的生物进化过程的计算模型，是一种通过模拟自然进化过程搜索最优解的方法。

基本遗传算法通过编码、适应度函数、遗传算子和运行参数的选择等，实现对自然进化的模拟。并且通过模式定理和收敛性理论解决模式的发现和算法的收敛性问题。模式定理反映了重要基因的发现过程，重要基因对应于较高的适应度值，说明了它们所代表的个体在下一代有较高的生存能力，是提高群体适应性的进化方向。而收敛性理论能够回答给定的一个

遗传算法执行策略是否收敛？它是进化到某个局部最优还是全局最优？如果一个遗传算法是收敛的，它需要多长时间收敛？但是，遗传算法的全局优化收敛性的理论分析尚未完全解决，基本遗传算法并不保证全局最优收敛，而只能在一定的约束条件下，实现全局最优收敛。

遗传算法是目前应用最广的优化搜索算法之一。但遗传算法存在收敛速度慢和易于陷入局部最优的问题，在需要优化的参数较多时，更凸显了遗传算法的不足。为了提高遗传算法跳出局部最优的能力和提高遗传算法的收敛速度，许多学者从不同的角度对遗传算法进行了改进，使遗传算法的寻优能力有了不同程度的提高。

参 考 文 献

[1] Holland J H. Adaptation in natural and artificial systems. The university of Michigan Press, 1975.

[2] Fogel L J. Evolutionary programming in perspective: The top-down view. In:Zurada J M, et al. eds. Computational Intelligence Imitating Life, New York: IEEE Press,1994.

[3] Fogel L J. Intelligence Through Simulated Evolution: Forty Years of Evolutionary Programming. A Wiley-Interscience Publication, 1999.

[4] Schwefel H P, Wegener I, Weinert K,eds. Advances in Computational Intelligence: Theory and Practice. Springer-Verlag.2003.

[5] De Jong K A. An Analysis of the Bchavior of a Class of Genetic of Genetic Adaptive Systems. Ph D Dissertation, University of Michigan, No.76-9381,1975.

[6] Godberg D E. Genetic Algorithms in Search, Optimization and Machine Learning. Addison-Wesley,1989.

[7] Davis L D. Handbook of Genetic Algorithms. Van Nostrand Remhold,1991.

[8] Koza J R. Genetic Programming, on the Programming of Computers by Means of Natural Selection. MIT Press,1992.

[9] Koza J R. Genetic Programming II, Automatic Discovery of Reusable Programs MIT Press,1994.

[10] 戴晓明，邹润民，冯瑞，张洪源，邵惠鹤．混合并行遗传算法求解 TSP 问题．电子与信息学报，2002,24(10):1424-1427.

[11] 赵宏立，庞小红，吴智铭．基因块编码的并行遗传算法及其在 TSP 中的应用．上海交通大学学报，2004,38(10)：213-217.

[12] 江雷．基于并行遗传算法的弹性 TSP 研究．微电子学与计算机.2005, 22(8)：130-134.

[13] 周明，孙树栋．遗传算法原理及应用．北京：国防工业出版社,2005,5．
[14] Goldberg D E. Genetic Algorithms in Search, Optimization, and Machine Learning, Readings .MA:Addison-Wesley,1989．
[15] 蔡自兴，徐光祐．人工智能及其应用．北京：清华大学出版社，2004．
[16] 李敏强等．遗传算法的基本理论与应用．北京：科学出版社，2002．
[17] Michalewics Z. Genetic Algorithms + Data Structure = Evolution Programs. Berlin: Springer Verlag, 1994．
[18] Michalewics Z, Attia N. Evolutionary Algorithms for Constrained Parameter Optimization Problems[R]. Technical Report, Dept. of Computer Science, Univ. of North Carolina,1994．
[19] Rudolph G. Convergence analysis of canonical genetic algorithm. IEEE Trans. on Neural Networks,1994,5(1):166-173．
[20] 武兆慧，张桂娟，刘希玉．基于模拟退火遗传算法的关联规则挖掘．计算机应用，2005,25(5)：1009-1011．
[21] Jeong II-Knon, Lee Ju-Jang. Adaptive Simulated Annealing Genetic Algorithm for Control Applications . International Journal of Systems Science, 1996,27(2):241-252．
[22] Bergy Paul K, Ragsdale Clifft, Hoskote Mangesh. A Simulated Annealing Genetic Algorithm for the Electrical Districting Problem. Annals of Operations Research,2003(121):33-35．
[23] Srinvas M,Patnaik L M.Adaptive Probabilities of Crossover and Mutation in Genetic Algorithms.IEEE Trans on Systems, Man and Cybernetics ,1994;24(4):656-667.
[24] Goldberg D E. Messy Genetic Algorithms: Motivation, Analysis and First Result. Complex Systems,1989:493-530．
[25] Cavichio D J. Reproductive Adaptive Plans. In:Proc. of the ACM 1972 Annual Conf,1972:1-11．
[26] Cavicchio D J. Adaptive Search Using Simulated Evolution. Ph D Dissertation, University of Michigan,1970．
[27] Glodberg D E, Richardson J. Genetic Algorithms with Sharing for Multimodal Function Optimization. In: Proc. of 2nd Int. Conf. on Genetic Algorithms, Lawrence Erlbaurn Associates, 1987:41-49．
[28] Joachim S. Parallel Genetic Algorithm: Theory and Application. ISO Press,1993．
[29] Petty C C, Lenze M R. A Theoretical Investigation of A Parallel Genetic Algorithm. In: Parallel problem Solving from Nature, Springer-Verlag, 1991．

Chapter 6

第6章 群体智能

作为一种新兴演化计算技术，群体智能已成为新的研究热点，它与人工生命，特别是进化策略和遗传算法有着极为特殊的联系，已完成的理论和应用研究证明群体智能方法是一种能够有效解决大多数全局优化问题的新方法。更为重要的是，群体智能的潜在并行性和分布式特点为处理大量的以数据库形式存在的数据提供了技术保证。目前,群体智能理论研究领域有两种主要的算法：粒子群优化算法（Particle Swarm Optimization，PSO） 和蚁群算法（Ant Colony Optimization，ACO）。蚁群算法是对蚂蚁群落食物采集过程的模拟，已成功应用于许多离散优化问题。粒子群优化算法也是起源于对简单社会系统的模拟，最初是模拟鸟群觅食的过程，但后来发现它是一种很好的优化工具。事实上，群体智能方法能够被用于解决大多数优化问题或能够转化为优化求解的问题。现在其应用领域已扩展到多目标优化、数据分类、数据聚类、模式识别、电信 QoS 管理、生物系统建模、流程规划、信号处理、机器人控制、决策支持，以及仿真和系统辨识等方面，群体智能理论和方法为解决这类应用问题提供了新的途径[1]。

6.1 粒子群优化算法

粒子群优化算法（Particle Swarm Optimization，PSO）是由 Eberhart 博士和 Kennedy 博士[2]共同提出的一种进化计算技术，是进化计算领域中的一个新的分支。该算法源于对鸟群、

鱼群觅食行为的模拟。在 PSO 中，首先初始化一群随机粒子（随机解），然后通过迭代寻找最优解。在每一次迭代中，粒子通过跟踪两个极值来更新自己的速度和位置。第一个就是粒子本身所找到的最优解，这个解叫做个体极值；另一个极值是整个种群目前找到的最优解，这个极值是全局极值，另外也可以不用整个种群而只是用其中一部分作为粒子的邻居，那么在所有邻居中的极值就是局部极值。PSO 算法简单易实现，不需要调整很多参数。

6.1.1　粒子群优化算法的基本原理

1．基本粒子群优化算法

粒子群优化算法和其他进化算法相似，也是根据对环境的适应度将群体中的个体移动到好的区域，因此有人认为它属于进化算法的一种。不同之处在于它不像其他进化算法一样对个体使用进化算子，而是将每个个体看做是 d 维搜索空间中的一个没有体积、没有质量的粒子，在搜索空间中以一定的速度飞行，并根据对个体和集体的飞行经验的综合分析来动态调整这个速度。

设群体中第 i 个粒子为 $\boldsymbol{X}_i(x_{i1},x_{i2},\cdots,x_{id})$，它经历过的位置为 $\boldsymbol{P}_i=(p_{i1},p_{i2},\cdots,p_{id})$，其中最佳位置为 pbest。当前组成群体的所有粒子经历过的最佳位置为 gbest。粒子 i 的速度用 $\boldsymbol{V}_i=(v_{i1},v_{i2},\cdots,v_{id})$ 表示。对每一次迭代，粒子 i 在 d 维（$1\leqslant d\leqslant D$）空间的运动遵循如下方程：

$$v_{id}^{k+1}=v_{id}^{k}+c_1*\text{Rand}()*(p_{id}-x_{id}^{k})+c_2*\text{Rand}()*(\text{gbest}^{k}-x_{id}^{k}) \tag{6.1}$$

$$x_{id}^{k+1}=x_{id}^{k}+v_{id}^{k} \tag{6.2}$$

其中，c_1 和 c_2 为加速常数（Acceleration Constants），它们使每个粒子向 pbest 和 gbest 位置加速运动。Rand()为[0,1]范围里变化的随机数。此外，粒子的速度 $\boldsymbol{V}_i$ 被限制为该维的最大速度 $\boldsymbol{V}_{\max}$。它决定了粒子在解空间的搜索精度，如果 $\boldsymbol{V}_{\max}$ 太高，则粒子可能会飞过最优解，如果 $\boldsymbol{V}_{\max}$ 太小，则粒子陷入局部搜索空间而无法进行全局搜索。

式（6.1）中的第一部分为粒子先前的速度，表示粒子对当前自身运动状态的信任，依据自身的速度进行惯性运动；第二部分为“认知”部分，表示粒子本身的思考，即一个得到加强的随机行为在将来出现的几率增大。这里的行为即“认知”，并假设获得正确的知识是得到加强的，从而实现一个增强学习过程。

第三部分为“社会”部分，表示粒子的信息共享与相互合作。“社会”部分可以通过 Bandura 的代理概念来理解[3]。根据该理论，当观察者观察到某一行为被加强时，将增加它实行该行为的几率，即粒子本身的认知将被其他粒子所模仿。微粒群算法的这些心理学假设是无争议

的：在寻求一致认知过程中，个体往往记住它们的信念，同时考虑同事的信念。当个体察觉同事信念较好的时候，它将进行适应性调整。

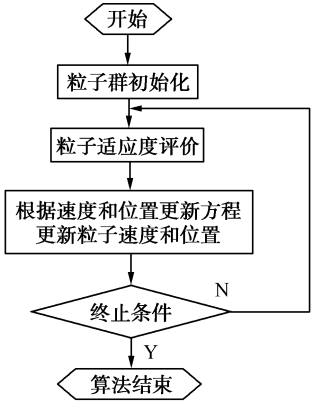


图 6.1 粒子群优化算法的流程图

根据 PSO 的基本原理，粒子群优化算法的流程图如图 6.1 所示。

（1）初始化：初始搜索点的位置 $\boldsymbol{X}_i^0$ 及其速度 $\boldsymbol{V}_i^0$ 通常是在允许的范围内随机产生的，每个粒子的 pbest 坐标设置为其当前位置，且计算出其相应的个体极值（即个体极值点的适应度值），而全局极值（即全局极值点的适应度值）就是个体极值中最好的，记录该最好值的粒子序号，并将 gbest 设置为该最好粒子的当前位置。

（2）评价每个粒子：计算粒子的适应度值，如果好于粒子当前的个体极值，则将 pbest 设置为该粒子的位置，且更新个体极值。如果所有粒子的个体极值中最好的好于当前的全局极值，则将 gbest 设置为该粒子的位置，记录该粒子的序号，且更新全局极值。

（3）粒子的更新：用式（6.1）和式（6.2）对每个粒子的速度和位置进行更新。

（4）检验是否符合终止条件：如果当前的迭代次数达到了预先设定的最大次数（或达到最小错误要求），则停止迭代，输出最优解，否则转到步骤（2）。

2．带惯性权重的粒子群优化算法

为了改善基本粒子群优化算法的收敛性能，Shi 和 Eberhart[4]在 1998 年的 IEEE 国际进化计算学术会议上发表了题为“A Modified Particle Swarm Optimizer”的论文，引入了惯性权重，大家都逐渐地默认这个改进的粒子群优化算法为标准的粒子群优化算法[5]。添加了惯性权重的速度更新公式为：

$$v_{id}^{k+1} = \omega * v_{id}^{k} + c_1 * \text{Rand}() * (p_{id} - x_{id}^{k}) + c_2 * \text{Rand}() * (\text{gbest}^{k} - x_{id}^{k}) \qquad (6.3)$$

参数 ω 对 PSO 能否收敛起重要作用，它使粒子保持运动惯性，使其有扩展搜索空间的趋势，有能力探索新的区域。ω 值大些有利于全局搜索，收敛速度快，但不易得到精确解；ω 值小些有利于局部搜索和得到更为精确的解，但收敛速度慢且有时会陷入局部极值。合适的 ω 值在搜索精度和搜索速度方面起协调作用。

为了观察惯性权重对粒子群优化算法性能的影响，Shi 和 Eberhart 把此算法应用到 Schaffer's $f6$ 函数中。通过大量的实验得出，惯性权重不应设定为定值，而应设为一个随时间线性减少的函数，惯性权重的函数形式通常为：

$$\omega = \omega_{\max} - \frac{\omega_{\max} - \omega_{\min}}{\text{iter}_{\max}} \times k \tag{6.4}$$

其中，$\omega_{\max}$ 为初始权重；$\omega_{\min}$ 为最终权重；$\text{iter}_{\max}$ 为最大迭代次数；k 为当前的迭代次数。

这个函数使得粒子群算法在刚开始的时候倾向于开掘，然后逐渐转向于开拓，从而在局部区域调整解。这些改进使得粒子群算法的性能得到了很大的提高。

6.1.2　改进的粒子群优化算法

粒子群优化算法是一种基于迭代的优化工具。但是在算法实现过程中没有交叉、变异操作，而是以粒子对解空间中最优粒子的追随进行解空间的搜索。同遗传算法相比，PSO 的优点在于流程简单易实现，算法参数简洁，无需复杂的调整。因此从出现至今，PSO 被迅速地应用于函数优化、神经网络训练、模糊系统控制、数据聚类，以及原有的一些遗传算法应用领域，作为一种新颖的优化搜索算法，研究者们的大部分精力主要集中于对其算法结构和性能的改善方面的研究，主要包括：参数设置、粒子多样性、种群结构和算法融合。

1．二进制离散粒子群优化算法

由于基本粒子群优化算法主要针对连续函数进行搜索运算，但许多实际工程问题都描述为离散的组合优化问题，为此 Kennedy 和 Eberhart 于 1997 年共同提出了一种二进制离散粒子群优化算法[6]。他们在提出的模型中将每一维 x_{id} 和 pbest_{id} 限制为 1 或 0，而速度 v_{id} 不做这种限制。由粒子速度决定一个范围在[0,1]之间的概率选择参数 s：若 s 接近于 1，则粒子将更可能被选择为 1；而若 s 接近于 0，则粒子更可能被选择为 0。Kennedy 等人提出使用 Sigmoid 函数来求参数 s。

Sigmoid 函数的表达式为：

$$s = \text{Sigmoid}(v_i^k) = \frac{1}{1 + \exp(-v_i^k)} \tag{6.5}$$

二进制离散粒子群优化算法的粒子速度和位置的更新公式为：

$$v_{id}^{k+1} = \omega * v_{id}^k + c_1 * \text{Rand}() * (x_{\text{pbest},i}^k - x_i^k) + c_2 * \text{Rand}() * (x_{\text{gbest}}^k - x_i^k) \tag{6.6}$$

$$x_i^{k+1} = \begin{cases} 1, & \rho < \text{Sigmoid}(v_i^{k+1}) \\ 0, & \text{otherwise} \end{cases} \tag{6.7}$$

其中，ρ 是[0,1]之间的随机数，算法中其他参数都和基本粒子群优化算法的参数相同。

2．参数改进与优化

PSO 算法与其他计算智能方法的一个显著区别就是所需调整的参数很少，但是这些关键参数的设置对算法的精度和效率却存在显著影响。

Shi 等人提出的带惯性权重的粒子群优化算法加快了收敛速度，提高了 PSO 算法的性能。当待解决问题很复杂时，该方法使得 PSO 在迭代后期全局搜索能力不足，导致不能找到要求的最优解[7]。为了弥补以上缺陷，Shi 等[8]人于 2001 年又提出用模糊控制器来动态自适应地改变惯性权重的技术。控制器的输入是当前惯性权重 ω 和当前最好性能评价值（CBPE），CBPE 衡量 PSO 目前找到的最好候选解的性能；输出是 ω 的改变量。由于不同的问题有不同范围的性能评价值，因此需要对 CBPE 进行如下的规范化：

$$\mathrm{NCBPE}=\frac{\mathrm{CBPE}-\mathrm{CBPE}_{\min}}{\mathrm{CBPE}_{\max}-\mathrm{CBPE}_{\min}} \tag{6.8}$$

NCBPE 是规范化后的评价值，$\mathrm{CBPE}_{\min}$ 和 $\mathrm{CBPE}_{\max}$ 依问题而定，且需要事先得知或可估计。

模糊权重法通过自适应模糊控制器能预测使用什么样的 ω 更合适，可以动态地平衡全局和局部搜索能力。但是由于需要知道 $\mathrm{CBPE}_{\min}$ 和 $\mathrm{CBPE}_{\max}$ 等，使得模糊权重法的实现较为困难，因而无法广泛使用[9]。

收缩因子法也是一种对参数进行改进和优化的粒子群算法。该方法由 Clerc[10,11]提出，通过加入收缩因子来保证 PSO 算法收敛，该算法由此也被称为收缩因子 PSO（CFPSO）。其表达式为：

$$v_{id}^{k+1}=\chi(v_{id}^{k}+c_1*\mathrm{Rand}()*(p_{id}-x_{id}^{k})+c_2*\mathrm{Rand}()*(\mathrm{gbest}^{k}-x_{id}^{k})) \tag{6.9}$$

其中，收缩因子为：

$$\chi=\frac{2}{|2-\phi-\sqrt{\phi^2-4\phi}|},\quad \phi=c_1+c_2,\quad \phi>4 \tag{6.10}$$

在使用收缩因子方法时，通常取 ϕ 为 4.1，从而使收缩因子 χ 等于 0.729。Clerc 在推导收缩因子法时，建议不再限制最大速度。但是，后来研究者发现设定最大速度限制可以提高算法的性能[12]。从数学上分析，惯性权值 ω 和收缩因子 χ 这两个参数是等价的[13]。

另外，El-Gallad A[14]针对算法中的种群规模、迭代次数和粒子速度的选择方法进行了详细分析，利用统计实验方法对约束优化问题的求解论证了这三个参数对算法性能的基本影响，并给出了具有一定通用性的三种参数选择原则。Fieldsend[15]利用 PSO 解决了多目标优化问题，分析了种群最优解、本地最优解、个体最优解对算法特性的影响，并通过对惯性权值加以扰动实现其动态调整以获取更佳的优化结果。

3．控制种群多样性的改进算法

为了避免算法过早收敛，一些研究者提出了通过控制种群多样性来提高算法总体性能的方法。Jacques Riget 和 Jakob S Vesterstrom[16]设计了一种以基本 PSO 为基础的，通过多样性度量控制种群特征，从而实现了粒子间吸引和互斥平衡以避免算法收敛性早熟的方法。这种方法在原有算法粒子间位置更新的相互吸引过程之后又引入了一个排斥过程，也就是吸引的逆过程，如式（6.11）所示：

$$v_{id}^{k+1}=\omega*v_{id}^{k}-c_1*\text{Rand}()*(p_{id}-x_{id}^{k})-c_2*\text{Rand}()*(\text{gbest}^{k}-x_{id}^{k}) \tag{6.11}$$

这种逆变过程在一定程度上抑制了吸引过程导致的系统多样性的下降。如果系统多样性下降至某个预定的指标，则将算法切换到互斥过程以增加粒子的多样性。当互斥过程使这种多样性恢复到预定的水平时，结束互斥操作继续基本算法运行。其中所需的多样性度量标准定义如下：

$$\text{diversity}(S)=\frac{1}{|S||L|}\sum_{i=1}^{|S|}\sqrt{\sum_{j=1}^{N}(p_{ij}-p_j)^2} \tag{6.12}$$

其中，$|S|$是种群的规模大小，$|L|$是搜索空间的最大对角线长度。N是问题的维数，p_{ij}是第 i 个粒子的第 j 个值，p_j是所有粒子第 j 个值的平均值。

Morten Lovbjerg 和 Thiemo Krink[17]提出了另一种改善粒子多样性的途径——自组织临界点控制（Self-Organized Criticality，SOC）方法。SOC 粒子与基本粒子的唯一区别就是每个粒子增加了当前临界值属性。每个粒子的临界值 C 初始化为零，如果两个粒子间的距离小于预定的距离阈值，则增加彼此的临界值。当某个粒子的临界值超过系统全局的极限值时，须重新分配其在解空间中的位置，如此便使粒子搜索的多样性得到了有效的增强。

同样是针对算法搜索多样性的问题，Thiemo Krink[18]等人提出了一种粒子空间扩展的方法（SPEPSO）来解决粒子间的冲突和聚集问题，并增强粒子突破局部极小值的能力。这种方法中为每个粒子附加一个最小独立半径 r，当与其他粒子间的距离小于 r 时，即认为二者发生“摩擦”，则采取控制措施使之分离。SPEPSO 还提出了粒子分离方向和速度的确定问题，并给出了三种基本策略：随机反弹、真实物理反弹、原始轨迹反弹。另外，通过反弹速度因子（0～1 之间取值）实现了对原速度的改变以防粒子冲撞。

4．小生境粒子群优化算法

2002 年 Brits 等人[19]将小生境技术引入粒子群优化算法中，提出了小生境粒子群算法（Niche PSO）。

基于小生境技术的 PSO 算法的基本思想是：对整个粒子群进行适当的划分，从而得到一些子粒子群；然后将子粒子群中的粒子以所在子粒子群中的最优粒子作为运动目标，进行进化。所以基于小生境技术的 PSO 优化算法的关键在于如何对整个粒子群进行适当的划分。

在 Brits 等人提出的小生境粒子群算法中，为保证粒子群的多样性，若某个粒子在运算连续多次迭代中对应的适应度值变化量很小，则以此粒子为中心，以此粒子与其最近的粒子的距离为半径构造一个圆形小生境。定义小生境的子粒子群的半径为：

$$R_{s_j} = \max\{\| \boldsymbol{x}_{s_j,g} - \boldsymbol{x}_{s_j,i} \|\} \tag{6.13}$$

其中，$x_{s_j,g}$、$x_{s_j,i}$ 分别为子粒子群 S_j 中的最优粒子和任一非最优粒子。算法有两个核心操作：

（1）若粒子 x_i 进入粒子群 S_j 范围内，即 $\| \boldsymbol{x}_i - \boldsymbol{x}_{s_j,g} \| \leqslant R_{s_j}$，则粒子将被此小生境粒子群吸收。

（2）若两个子粒子群 S_j、S_k 范围相交，即 $\| \boldsymbol{x}_{s_j,g} - \boldsymbol{x}_{s_j,k} \| \leqslant | R_{s_j} - R_{s_k} |$，则两个子粒子群将被合并成一个。

小生境粒子群优化算法的具体步骤如下。

（1）设置算法参数，初始化粒子群。

（2）使用单认知模型（Cognition-only Model）的粒子群优化算法对主粒子群进行一次搜索运算，并计算新粒子群的适应度值。

（3）对于每个子粒子群进行以下操作。

① 使用一般收敛粒子群算法（GCPSO）的更新式（6.14）和式（6.15）来更新粒子：

$$v_i^{k+1} \leftarrow -x_{\text{gbest}}^k + x_{\text{pbest},i}^k + \omega v_{\text{gbest}}^k + \eta^k (1 - 2r_2^k) \tag{6.14}$$

$$x_i^{k+1} \leftarrow x_{\text{pbest},i}^k + \omega v_{\text{gbest}}^k + \eta^k (1 - 2r_2^k) \tag{6.15}$$

其中，η为搜索范围的最大值。

② 计算每个子粒子群的适应度值。

③ 更新子粒子群小生境的半径。

（4）如果可能的话，根据操作①合并符合要求的子粒子群。

（5）如果可能的话，根据操作②吸收符合要求的粒子。

（6）重复步骤（2）直到到达最大迭代次数或结果满足要求。

除了上面的小生境粒子群优化算法以外，也有许多学者把小生境粒子群算法与其他的方法相结合，提出了新的小生境粒子群优化算法。贾东立等人[20]结合小生境策略全局优化与变尺度混沌变异精细搜索各自的优点，提出了一种全新的粒子群优化算法，并在算法中引入了种群淘汰策略，结合小生境的子种群竞争策略一起作用。运行中首先利用 RCS（Restricted Competition Selection）[21]竞争策略，使各个小生境子种群形成独立的搜索空间，追逐不同的

极值点；然后每隔一定代数，对陷入局部最优的最劣子种群进行随机初始化。这样可使种群在不断的竞争和更新中向前进化，从而避免了算法早熟收敛，保证了收敛到全局最优。而没有更新的小生境种群继续向前进化，又保证了搜索进度的连续提高。

刘健辰等人[22]在分析已有的标准 PSO 优化算法及其改进算法的基础上，提出了一种基于聚类分析的小生境粒子群算法。该算法根据粒子在解空间分布的结构特征，首先采用基于密度的聚类分析方法构造初始粒子群，形成小生境，然后通过限制粒子的进化仅仅在小生境内进行，小生境之间不存在信息交流，达到保持种群多样性的目的。

5．混合粒子群优化算法

在进化算法研究中，算法的探测（Exploration）和开发（Exploitation）能力单靠一种算法往往无法得到有效利用与平衡，从而影响了算法的求解精度和效率。所以人们想到了将两种算法或多种算法混合在一个模型当中，尽量发挥各个算法的优点，从而形成了一个研究混合算法的方向。

1）基于遗传思想的改进粒子群算法

Angeline[23]提出了用进化计算中的选择机制来改善粒子群优化算法。Angeline 提出的混合群体（Hybrid Swarm）结合了类似于传统进化计算算法中的选择机制。除结合了进化计算中的锦标选择算子以外，混合群体和粒子群在各方面都很相似。选择过程在粒子修改群体前执行。通过增加这个选择过程，在每一代中，一半的个体将会被移动到比当前位置具有相对优势的位置上。移动后的个体将仍然保持它们的个体最优位置。

Lovbjerg[24]提出了繁殖粒子群算法，粒子群中的粒子被赋予一个杂交概率，这个杂交概率由用户定义，与粒子的适应度值无关。在每次迭代中，根据杂交概率选择一定数量的粒子进入一个池中，池中的粒子随机地两两杂交，产生相同数目的子代，并用子代粒子取代父代粒子，以保证种群的粒子数目不变。通过该方法产生的子代代替父代，选择父代不基于适应度值，防止了基于适应度值的选择对那些多局部极值的函数带来潜在问题。

2）混沌粒子群优化算法

混沌（Chaos）是自然界中一种常见的非线性现象。混沌变量看似杂乱的变化过程其实含有内在的规律性，利用混沌变量的随机性、遍历性及规律性可以进行优化搜索。

一般将由确定性方程得到的具有随机性的运动状态称为混沌，呈现混沌状态的变量称为混沌变量。如下的 Logistic 方程[25]是一个典型的混沌系统：

$$z_{n+1} = \mu z_n (1 - z_n) \qquad n = 0,1,2,\cdots \tag{6.16}$$

式中，μ 为控制参量，方程可以看做是一个动力学系统。μ 值确定后，由任意初值 $z_0 \in [0,1]$，可以迭代出一个确定的时间序列 $z_1, z_2, z_3, \cdots$。一个混沌变量在一定范围内有如下特点：随机

性，即它的表现同随机变量一样杂乱；遍历性，即它可以不重复地历经空间内的所有状态；规律性，该变量是由确定的迭代方程导出的。混沌优化方法利用混沌系统特有的遍历性来实现全局最优，而且它不要求目标函数具有连续性和可微性的性质。

通过分析粒子群优化算法的缺点和混沌优化具有遍历性的优点，参考文献[26]、[27]提出了混沌粒子群优化算法。算法的主要措施是利用混沌运动的遍历性以当前整个粒子群迄今为止搜索到的最优位置为基础产生混沌序列，把产生的混沌序列中的最优位置粒子随机替代当前粒子群中的一个粒子的位置。该算法的具体步骤如下。

（1）确定参数：基本粒子群算法中的加速常数 c_1 和 c_2，群体规模 N，进化次数，混沌寻优次数。

（2）随机产生 N 个粒子的种群。

（3）按照基本粒子群算法的式（6.1）和式（6.2）对粒子进行操作。

（4）对最优位置 $\boldsymbol{p}_g=(p_{g,1},p_{g,2},\cdots,p_{g,n})$ 进行混沌优化。将 $p_{g,i}(i=1,2,\cdots,n)$ 映射到 Logistic 方程的定义域[0,1]：$z_i=\dfrac{p_{g,i}-a_i}{b_i-a_i},(i=1,2,\cdots,n)$，然后用 Logistic 方程进行迭代产生混沌变量序列 $z_i^{(m)}(m=1,2,\cdots)$，再把产生的混沌变量序列 $z_i^{(m)}(m=1,2,\cdots)$ 通过逆映射 $p_{g,i}^{(m)}=a_i+(b_i-a_i)z_i^{(m)}(m=1,2,\cdots)$ 返回到原解空间，得：

$$\boldsymbol{p}_g^{(m)}=(p_{g,1}^{(m)},p_{g,2}^{(m)},\cdots,p_{g,n}^{(m)}),\quad (m=1,2,\cdots) \tag{6.17}$$

在原解空间对混沌变量经历的每一个可行解 $\boldsymbol{p}_g^{(m)}(m=1,2,\cdots)$ 计算其适应度值，保留性能最好的可行解 $\boldsymbol{p}^*$。

（5）随机从当前群体中选择出一个粒子用 $\boldsymbol{p}^*$ 取代。

（6）若达到最大代数或得到满意解，则优化过程结束，否则返回步骤（3）。

上面的混沌粒子群优化算法采用的是混沌系统 Logistic 映射。而参考文献[28]提出的混沌粒子群混合优化算法采用的是一种自定义的正弦混沌映射，该映射构成混沌系统的遍历性要更好[29]。其混沌映射为：

$$z_{n+1}=\sin(5.65/z_n)，\ -1\leqslant z_n\leqslant 1,\quad z_n\neq 0 \tag{6.18}$$

迭代的初始值 z_0 不能为 0，且 z_0 不能取为无穷多个平衡点的任何一点，否则不能产生混沌，平衡点为方程 $z=\sin(5.65/z)$ 的解。

该算法通过分析混沌和 PSO 的特点，充分利用各自优势将两种机制有机结合，按粒子搜索方式不同将整个粒子群体分为两个分群，分别命名为 PSO 分群（P 群）和混沌分群（C 群）。优化过程分为两个阶段，第一阶段 P 群和 C 群分别按 PSO 搜索机制和混沌遍历机制迭代，其中 P 群粒子速度更新方程中 gbest 为整个粒子群体而不是本分群 t 时刻全局最优解，利用混沌

优化算法的全局遍历性避免“早熟”；第二阶段 P 群粒子收敛于局部极值点，此时 C 群粒子以局部极值点为中心进行混沌迭代，同时将 C 群的适应度值较好的部分粒子替换 P 群中数量相同的较差粒子，帮助 P 群粒子逃离局部最优区。

3）基于模拟退火的粒子群优化算法

模拟退火算法（Simulate Anneal Arithmetic，SAA）由 Kirkpatrick[30]在 1983 年首次提出。算法源于固体退火原理，模拟了高温金属降温的热力学过程。

2004 年高鹰等人[31]提出了以基本粒子群优化算法作为主体运算流程，引入模拟退火机制，并混合了基于遗传思想的粒子群优化算法中的杂交运算和带高斯变异的粒子群优化运算的模拟退火粒子群优化算法（Simulate Anneal-Particle Swarm Optimization，SA-PSO）。算法首先随机产生一个初始粒子群，然后通过基本粒子群优化算法对初始粒子群进行搜索，产生一个较优的新粒子群。再应用杂交算法和带高斯变异算法在模拟退火操作下对这个较优的粒子进行寻优运算，最终得到算法结果。

6.1.3　粒子群优化算法的应用

粒子群算法作为新兴群体智能算法，自从提出之后，由于其概念简明、实现方便，在短期内迅速得到了国际进化计算研究领域的认可，并且由于其在解决复杂的组合优化类问题方面所具有的优越性能，因而被广泛地应用于神经网络训练、数据挖掘等领域。

1．组合优化问题

TSP 是运筹学、图论和组合优化中的 NP 难题，常被用来验证智能启发式算法的有效性。TSP 问题描述非常简单，但最优化求解很困难，若用穷举法搜索，则要考虑所有可能情况，并两两对比，找出最优，其算法复杂性呈指数增长，即所谓的“组合爆炸”。所以寻求和研究 TSP 的有效启发式算法，是问题的关键。

PSO 算法虽然成功地应用在连续优化问题中，但在组合优化问题中的研究和应用还很少。参考文献[32]通过引入交换子和交换序的概念，对基本 PSO 算法进行改造，并将其应用于求解 TSP 问题中。

该方法首先定义了交换子和交换序。交换子用来交换 TSP 问题的解序列中点之间的顺序；交换序是一个或多个交换子的有序队列。交换序作用于一个 TSP 解上意味着这个交换序中的所有交换子依次作用于该解上。

该方法还对基本 PSO 算法中的速度算式进行了重新构造：

$$V'_{\mathrm{id}} = V_{\mathrm{id}} \oplus \alpha(P_{\mathrm{id}} - X_{\mathrm{id}}) \oplus \beta(P_{\mathrm{gd}} - X_{\mathrm{id}}) \tag{6.19}$$

其中，$\oplus$ 为两个交换序的合并算子；$\alpha,\beta(\alpha,\beta\in[0,1])$ 为随机数，$\alpha(P_{\mathrm{id}}-X_{\mathrm{id}})$ 表示基本交换序 $(P_{\mathrm{id}}-X_{\mathrm{id}})$ 中的所有交换子以概率 α 保留；同理 $\beta(P_{\mathrm{gd}}-X_{\mathrm{id}})$ 表示基本交换序 $(P_{\mathrm{gd}}-X_{\mathrm{id}})$ 中的所有交换子以概率 β 保留。由此可以看出，α 的值越大，$(P_{\mathrm{id}}-X_{\mathrm{id}})$ 保留的交换子就越多，P_{id} 的影响就越大；同理 β 的值越大，$(P_{\mathrm{gd}}-X_{\mathrm{id}})$ 保留的交换子就越多，P_{gd} 的影响就越大。

求解 TSP 问题的 PSO 算法步骤描述如下。

（1）初始化粒子群，即给群体中的每个粒子赋一个随机的初始解和一个随机的交换序。

（2）如果满足结束条件，转步骤（5）。

（3）根据粒子当前位置 X_{id}，计算其下一个位置 X'_{id}，即新解。

① 计算 P_{id} 和 X_{id} 之间的差 A，$A=P_{\mathrm{id}}-X_{\mathrm{id}}$，其中 A 是一个基本交换序，表示 A 作用于 X_{id} 得到 P_{id}。

② 计算 $B=P_{\mathrm{gd}}-X_{\mathrm{id}}$，其中 B 也是一基本交换序。

③ 根据式（6.19）计算速度 V'_{id}，并将交换序 V'_{id} 转换为一个基本交换序。

④ 计算搜索到的新解：

$$X'_{\mathrm{id}}=X_{\mathrm{id}}+V_{\mathrm{id}} \tag{6.20}$$

⑤ 如果找到一个更好的解，则更新 P_{id}。

（4）如果整个群体找到一个更好的解，更新 P_{gd}，转步骤（2）。

（5）显示求出的结果值。

通过用 14 个点的 TSP 标准问题对算法进行验证表明，算法只搜索了一个很小的区域就得到了一个已知最好的解，收敛速度很快。这表明算法是有效的。

2．神经网络训练

PSO 用于神经网络训练，主要包含 4 个方面：连接权重、网络拓扑结构及传递函数、学习算法[33]。每个粒子包含神经网络的所有参数，通过迭代来优化这些参数，从而达到训练的目的。与传统的误差反向传播（Back-Propagation，BP）算法相比，使用 PSO 训练神经网络的优点在于不使用梯度信息，而使用一些不可微的传递函数。多数情况下其训练结果优于 BP 算法，而且训练速度非常快。

基于粒子群的神经网络训练算法是在优化连接结构的同时结合传统 PSO 算法训练神经网络的连接权值。用来优化神经网络连接结构的 PSO 算法模型如下。

（1）连接变量速度的迭代：

$$v_{\mathrm{ih}}=w*v_{\mathrm{ih}}+c_1*\mathrm{Rand}(\,)*(p_i-\delta_{\mathrm{ih}})+c_2*\mathrm{Rand}(\,)*(g-\delta_{\mathrm{ih}}) \tag{6.21}$$

$$v_{\mathrm{ho}} = w * v_{\mathrm{ho}} + c_1 * \mathrm{Rand}(\,) * (p_i - \delta_{\mathrm{ho}}) + c_2 * \mathrm{Rand}(\,) * (g - \delta_{\mathrm{ho}}) \tag{6.22}$$

其中，δ_{ih} 和 δ_{ho} 是连接变量，一般为[0,1]区间的实数。

（2）连接变量位置的迭代：

$$\delta_{\mathrm{ih}} \leftarrow \delta_{\mathrm{ih}} + v_{\mathrm{ih}} \tag{6.23}$$

$$\delta_{\mathrm{ho}} \leftarrow \delta_{\mathrm{ho}} + v_{\mathrm{ho}} \tag{6.24}$$

（3）连接结构的迭代：

$$\text{If}\ \ (\theta_{\mathrm{ih}} / \theta_{\mathrm{ho}} < \delta_{\mathrm{ih}} / \delta_{\mathrm{ho}}) \quad \text{Then} \quad c_{\mathrm{ih}} / c_{\mathrm{ho}} \leftarrow 1 \qquad \text{Else}\ \ c_{\mathrm{ih}} / c_{\mathrm{ho}} \leftarrow 0 \tag{6.25}$$

其中，θ_{ih} 和 θ_{ho} 是连接阈值，为[0,1]区间的实数，与连接变量结合用于控制神经网络的连接结构。c_{ih} 表示输入层与隐含层间的连接结构；c_{ho} 表示隐含层与输出层间的连接结构。c_{ih} 与 c_{ho} 均为二进制变量矩阵。对应的连接存在则该变量为 1，否则为 0。

优化连接结构的 PSO 算法模型中的连接变量速度—位置迭代公式为 PSO 算法的基本搜索模型。但是与传统 PSO 算法不同，该算法中 p_i, g 分别表示连接变量（而非连接结构本身）的个体与全局极值，由连接变量及阈值确定的连接结构结合基本 PSO 算法训练的连接权值在给定样本下的训练误差精度决定。该算法通过间接优化可连续变化的连接变量达到训练二进制表达的连接结构的目的，并由连接结构的迭代式（6.25）体现 PSO 算法对神经网络结构的更新。

3．在数据挖掘中的应用

分类和聚类是数据挖掘中比较重要的两个挖掘任务。由于 PSO 算法流程简单易实现，算法参数简洁，无需复杂的调整，因此，近几年来 PSO 也被应用来解决数据挖掘的任务。

参考文献[34]在编码分类规则和定义分类规则适应度的基础上，提出了基于 PSO 的分类规则提取算法。

1）分类规则编码

粒子群分类规则编码以每个粒子表示一条规则，规则集对应某个粒子群。每个粒子由不同的维度（定义为整数）组成，数据集 D 中每个特征属性对应粒子的不同维度值。数据集中的类别属性也对应粒子的一个维度值，但不参与粒子间的信息交换，属于粒子的恒定属性。对于一条分类规则，首先按照密歇根编码方案编码为按特征属性分段的二进制串，然后将每段二进制串转化为十进制数，作为粒子的不同维度。通过该方法，分类规则可以表达为一个粒子，任一粒子也与某个规则唯一对应。

2）分类规则适应度计算

假设规则 R 是关于类别 C 的一条分类规则。$T_{\text{pos}}(R)$ 表示在数据集中被规则覆盖的类别为 C 的样本数；$C_{\text{pos}}(R)$ 表示数据集中类别为 C 的样本数；$T_{\text{neg}}(R)$ 表示在数据集中被规则覆盖的类别不为 C 的样本数；$C_{\text{neg}}(R)$ 表示数据集中类别不为 C 的样本数；θ_1，θ_2 为[1,2]之间的实数。则分类规则适应度计算公式为：

$$f(R)=(\theta_1\times\frac{T_{\text{pos}}(R)}{C_{\text{pos}}(R)})\times(\theta_2\times\frac{T_{\text{neg}}(R)}{C_{\text{neg}}(R)}) \tag{6.26}$$

在算法过程中，取 $\theta_2>\theta_1$。

3）粒子群分类器

通过分类规则的粒子群编码和分类规则适应度的定义，在修改粒子群算法中粒子位置更新方程，并应用序列覆盖算法逐步挖掘数据集中分类规则的基础上，采用信任分配算法使得规则集对数据进行分类，最终实现基于粒子群算法的分类器设计。

参考文献[35]在 K-means 算法的基础上，提出了解聚类问题的基本粒子群算法。用 K 个聚类中心 $X=(m_{11},m_{12},\cdots,m_{1n},m_{21},m_{22},\cdots,m_{2n},\cdots,m_{k1},\cdots,m_{kn})$ 作为聚类问题的解，步骤如下。

（1）设定粒子数 n_p，规定迭代次数 $n_{\max}$，随机产生 n_p 个初始解 X_0。

（2）根据当前位置，以 $\min\sum_{j=1}^{K}\sum_{\boldsymbol{Y}\in S_j}\|\boldsymbol{Y}-\boldsymbol{m}_j\|$（$\boldsymbol{Y}$ 为样本集，S_j 表示 K 个聚类，$\boldsymbol{m}_j$ 为 j 类样本的均值向量）计算适应度值 l_0，设置当前适应度值为个体极值 plbest，当前位置为个体极值位置 pxbest，根据各个粒子的个体极值 plbest，找出全局极值 glbest 和全局极值位置 gxbest。

While（迭代次数<规定迭代次数 $n_{\max}$）do

for j=1: n_p

① 按照式（6.1）和式（6.2）更新速度和当前的位置，并且速度限制在 $v_{\max}$ 内。

② 根据当前位置，各个样本按最小距离原则分配给 K 个聚类中心。

③ 计算适应度值 l_1。

④ 如果 $l_1(j)<\text{plbest}(j)$，则 $\text{pxbest}(j)=X_1(j)$，$\text{plbest}(j)=l_1(j)$。

End;

⑤ 根据各个粒子的个体极值 plbest，找出全局极值 glbest 和全局极值位置 gxbest。

⑥ $X_0\leftarrow X_1$。

End。

（3）最后输出全局极值 glbest 和全局极值位置 gxbest。

纵观国内外粒子群算法的研究和应用现状，PSO 的研究发展趋势如下[36]。

（1）算法的理论分析。虽然微粒群算法在实际应用中被证明是有效的，但其算法分析还不成熟和系统。目前还没有给出收敛性、收敛速度估计等方面的数学证明，已有的工作还远远不够。

（2）粒子群拓扑结构。不同的粒子群邻居拓扑结构是对不同类型社会的模拟，研究不同拓扑结构的适用范围，对 PSO 算法推广和使用有重要意义。

（3）参数选择与优化。参数 w,c_1,c_2 的选择分别关系粒子速度的 3 个部分（惯性部分、社会部分和自身部分）在搜索中的作用。如何选择、优化和调整参数，使得算法既能避免早熟又能比较快速地收敛，对工程实践有着重要意义。

（4）与其他优化算法的融合。遗传算法、模拟退火算法等算法在不同的理论分析方面及应用领域方面各有千秋。粒子群算法只有通过与其他优化算法的比较，将其优点通过与自身优点相结合，扬长避短，才能提高算法的性能。

（5）算法应用。算法的研究是为了应用，算法的有效性必须在应用中才能体现，而应用对深化算法有着非常重要的意义。目前，PSO 的应用大量局限于连续、单目标、无约束的确定性优化问题。因此，如何将 PSO 算法应用于离散、多目标、约束、不确定、动态等优化问题，将是粒子群算法的主要研究方向。

6.2　蚁群算法

蚁群算法（Ant Colony Algorithm）是一种模拟进化算法。蚂蚁是一种众所周知的小昆虫，然而蚂蚁作为群体却表现出十分独特的生物特征和生命行为。20 世纪 90 年代初期，意大利学者多里戈、马尼佐和科洛龙等人从生物进化和仿生学角度出发，研究蚂蚁寻找路径的自然行为，提出了蚁群算法，并用该方法求解 TSP 问题、二次分配问题和作业调动问题，取得了较好的结果。蚁群算法已显示出它在求解复杂优化问题特别是离散优化问题方面的优势，是一种很有发展前景的计算智能方法。

6.2.1　蚁群算法的原理

作为与遗传算法属同一类的通用型随机优化方法，蚁群算法不需要任何先验知识，最初只是随机地选择搜索路径，随着对解空间的“了解”，搜索变得有规律，并逐渐逼近直至最终达到全局最优解[1]。蚁群算法对搜索空间的“了解”机制主要包括 3 个方面[37]。

（1）蚂蚁的记忆。一只蚂蚁搜索过的路径在下次搜索时就不会再被选择，由此在蚁群算法中建立 tabu（禁忌）列表来进行模拟。

（2）蚂蚁利用信息素（Pheromone）进行相互通信。蚂蚁在所选择的路径上会释放一种叫做信息素的物质，当同伴进行路径选择时，会根据路径上的信息素进行选择，这样信息素就成为蚂蚁之间进行通信的媒介。

（3）蚂蚁的集群活动。通过一只蚂蚁的运动很难到达食物源，但整个蚁群进行搜索就完全不同。当某些路径上通过的蚂蚁越来越多时，在路径上留下的信息素数量也越来越多，导致信息素强度增大，蚂蚁选择该路径的概率随之增加，从而进一步增加该路径的信息素强度；而某些路径上通过的蚂蚁较少时，路径上的信息素就会随时间的推移而蒸发。因此，模拟这种现象即可利用群体智能建立路径选择机制，使蚁群算法的搜索向最优解推进。图 6.2 说明了蚁群的路径搜索原理和机制[38]。

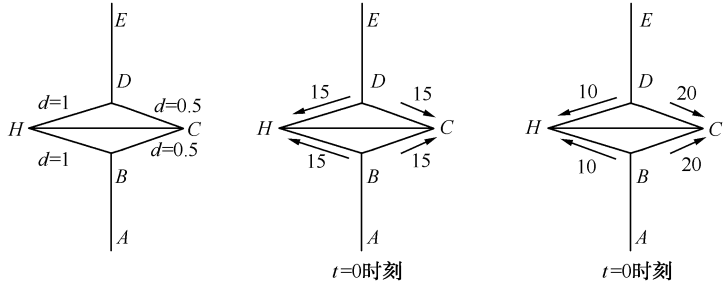


图 6.2　蚁群的路径搜索原理和机制

如图 6.2 所示，设 A 是蚂蚁的巢穴，E 是食物源，HC 为一障碍物。由于存在障碍物，蚂蚁只能绕经 H 或 C 由 A 到达 E，或由 E 到达 A。各点之间的距离如图 6.2 所示。设每个时间单位有 30 只蚂蚁由 A 到达 B，又有 30 只蚂蚁由 E 到达 D，蚂蚁过后留下的外激素为 1。为便于讨论，设外激素停留的时间为 1。在初始时刻，由于路径 BH，BC，DH，DC 上均无信息存在，位于 B 和 D 的蚂蚁可以随机选择路径。从统计的角度可以认为它们以相同的概率选择 BH，BC，DH，DC。经过一个时间单位后，在路径 BCD 上的信息量是路径 BHD 上的信息量的两倍。在 t=1 时刻，将有 20 只蚂蚁由 B 和 D 到达 C，有 10 只蚂蚁由 B 和 D 到达 H。随着时间的推移，蚂蚁将会以越来越大的概率选择路径 BCD，最终完成选择路径 BCD，从而找到由蚁巢到食物源的最短路径。由此可见，蚂蚁个体之间的信息交换是一个正反馈过程。

基本的蚁群算法模型由下面 3 个公式描述[39]。在搜索周期的第 t 代，蚂蚁个体 A_k 由城市 i 转移到城市 j 的概率 p_{ij}^k 定义为：

$$P_{ij}^k(t)=\begin{cases}\dfrac{\varphi_{ij}^{\alpha}(t)\eta_{ij}^{\beta}(t)}{\sum_{s\in W^k}\varphi_{is}^{\alpha}(t)\eta_{is}^{\beta}(t)} & j\in W^k\\ 0 & \text{其他}\end{cases} \tag{6.27}$$

其中，W^k 是蚂蚁 k 下一步允许选择的城市。

随着时间的推移，以前留下的信息素逐渐消逝，用参数 $1-\rho$ 表示信息消逝的程度，经 n 个城市的搜索，蚂蚁完成一次循环，各路径上的信息量要根据式（6.28）和式（6.29）做调整：

$$\varphi_{ij}(t+1)=\rho*\varphi_{ij}(t)+(1-\rho)\Delta\varphi_{ij}(t) \tag{6.28}$$

$$\Delta\varphi_{ij}(t)=\begin{cases}\dfrac{Q}{L_k} & \text{若第 } k \text{ 只蚂蚁在本次循环中经过 } ij\\ 0 & \text{其他}\end{cases} \tag{6.29}$$

其中，t 为迭代次数；i 为蚂蚁所在位置；j 和 s 为蚂蚁可以到达的位置；η_{ij} 为启发性信息，这里为由 i 到 j 的路径的能见度，即 $1/d_{ij}$；L_k 为目标函数，这里为两点间欧氏距离；φ_{ij} 是 i 到 j 的路径的信息素强度；$\Delta\varphi_{ij}^k$ 为蚂蚁 k 由 i 到 j 的路径上留下的信息素数量；α 为路径权；β 为启发性信息的权；ρ 为路径上信息素数量的蒸发系数；Q 为信息素质量系数。

搜索开始时，各条路径上分布的信息素相等，即 $\varphi_{ij}(0)=C$（C 为参数）。然后在搜索周期的每一代，通过信息素的蒸发作用和一些蚂蚁各条路径搜索带来的信息素增强作用来改变信息素值的大小。蚂蚁个体在搜索过程中，根据各条路径上的信息量决定前进的方向，在各节点处向下一节点的转移概率 P_{ij}^k 由信息素 φ_{ij} 和启发性信息 η_{ij} 共同决定。因此，蚂蚁个体依转移概率偏向于选择连接弧最短、具有高信息素值的位置来作为下一个搜索节点。

6.2.2　改进型蚁群算法

前面介绍的是基本蚁群算法。基本蚁群算法具有鲁棒性强、能够进行分布计算和易于与其他方法结合等优点。但是它还具有以下缺点。

（1）需要较长的计算时间，容易出现停滞现象。

（2）根据式（6.29），所有通过路段（i，j）的搜索路径对应的候选解均会对该路段带来信息素的增量。而实际上，候选解并非都是最好解，这样计算信息素的增量会导致错误的引导信息，从而造成大量的无效搜索，使系统出现停滞现象。

（3）式（6.29）中，采用了信息素均匀分配策略，即对已搜索路径中的所有路段采用同样的信息素增量，与路段的重要性无关。没有考虑当连续空间优化问题转换到有向图搜索问题时，信息素分配给可行解带来的尺度变化对于连续解空间搜索效率的影响。

鉴于基本蚁群算法的这些缺点，人们提出了许多改进的蚁群算法。

1．具有随机扰动特征的蚁群算法[40]

蚁群算法的主要依据是信息正反馈原理和某种启发式算法的有机结合。基本蚁群算法模型中的转移概率式（6.27）揭示了这一原理。它表明如果放到某条路径上的信息素越多且路径越短，那么该路径被蚂蚁选中的概率就越大。基于这样的原理，具有随机扰动特性的蚁群算法提出了更为简洁的转移策略：

$$P_{ij}^{k}=(\varphi_{ij}^{k}\eta_{ij}^{k})^{\gamma},\quad j\notin \mathrm{tatu}(k) \tag{6.30}$$

其中，$\gamma>0$ 为扰动因子，$\mathrm{tatu}(k)(k=1,2,\cdots,m)$ 用以记录蚂蚁 k 所走过的城市，并随时间做动态调整。需要指出的是，P_{ij}^{k} 不再是转移概率而是转移系数。蚂蚁总是选择转移系数最大的一条路径。为了避免算法运行中的停滞现象，扰动因子在算法中是可变的，并采用倒指数关系曲线来描述：

$$\gamma=a*\mathrm{e}^{b/k}(k=1,2,3,\cdots,M),\quad a>0,b>0 \tag{6.31}$$

其中，M 为最大迭代次数；a,b 为扰动尺度因子。不失随机性，令 $a=a'X$，其中 $a'>0$，X 是[0,1]上均匀分布的随机数。由式（6.31）可知，随着迭代次数的增大，γ 的值最终趋近于系数 a，而系数 b 的大小决定了曲线趋近于系数 a 的快慢程度。同时，为了避免最优的一条路径可能被漏选，在该算法中，还设计了一系列的扰动策略。通过扰动策略的设计，可以使该算法最终能找到全局最优解。

2．基于信息素扩散的蚁群算法[41]

蚂蚁个体在通过一条路径的过程中，要释放一定浓度的信息素。对于蚂蚁所释放出的信息素，基本蚁群算法仅仅考虑了其对该条路径的信息素浓度的影响，即增加了该条路径上的信息素浓度，同时也增加了其他蚂蚁选择这条路径的概率。但是，基本算法并没有考虑这些信息素对相邻路径信息素浓度的影响，即没有考虑信息素的扩散。通过研究发现，在自然界真实蚁群行为中，蚂蚁之间的信息传递主要是通过信息素的扩散完成的，先前的蚂蚁对后面的蚂蚁的行为发生影响时，后面的蚂蚁一般不在先前蚂蚁的运动轨迹上，而是与该运动轨迹有着或大或小的距离，当距离比较小时，后面的蚂蚁的行为受影响较大，当距离比较大时，后面蚂蚁的行为受影响较小。这就是基于信息素扩散的蚁群算法的基本思想。

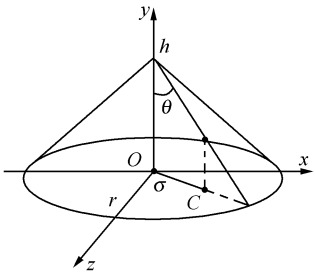


图 6.3　信息素扩散模型

在该算法中，建立了信息素扩散模型，如图 6.3 所示。

在信息素扩散模型中，O 点的信息素浓度为 $D_{\max}$，θ 参数为

锐角，在基于信息素扩散的蚁群算法模型中保持不变，h 是圆锥体的高，r 表示扩散范围的半径，其大小为 $h \cdot \mathrm{tg}\theta$，以图 6.3 中的 C 点为例，在该点的蚂蚁所接收到的信息素的浓度 D_c 用式（6.32）描述，其中 σ 表示 C 点到 O 点的距离。

$$D_c = D_{\max} * ((h * \mathrm{tg}\theta - \sigma)/(h * \mathrm{tg}\theta)) \tag{6.32}$$

从式（6.32）可以看出距离信息源越远，蚂蚁所接收到的信息素越少。

用基于信息素扩散的蚁群算法解决 TSP 问题时，假定蚂蚁 k 刚走过的两个城市 i 和 j 之间的距离为 d_{ij}，认为此时该蚂蚁将分别以 i 和 j 为中心向周围扩散信息素，其中 i 点和 j 点的信息素的浓度都为 $D_{\max}$，扩散的结果将形成形状与图 6.3 中的圆锥体类似的分别以 i 和 j 为底面中心的圆锥体（简化的浓度场），对于其他的任一城市 l，如果它在蚂蚁 k 所产生的信息素的扩散范围内，则能求出扩散到该城市的由蚂蚁 k 所产生的信息素的浓度 D^k_{il} 和 D^k_{jl}，这里直接用 D^k_{il} 和 D^k_{jl} 去更新路径 il 和 jl 上的信息素的浓度，这样就得到了第 k 只蚂蚁在一次循环中留在各有关路径上的信息素的浓度的计算公式，分别如式（6.33）～式（6.37）表示：

$$\Delta C^k_{ij} = Q / d_{ij} \quad \text{第 } k \text{ 只蚂蚁在时刻 } t \text{ 到 } t+1 \text{ 之间经过 } ij \tag{6.33}$$

$$\Delta C^k_{il} = D^k_{il} \quad \text{第 } k \text{ 只蚂蚁在时刻 } t \text{ 到 } t+1 \text{ 之间经过 } i \text{ 但不经过 } l \tag{6.34}$$

$$\Delta C^k_{jl} = D^k_{jl} \quad \text{第 } k \text{ 只蚂蚁在时刻 } t \text{ 到 } t+1 \text{ 之间经过 } j \text{ 但不经过 } l \tag{6.35}$$

$$D^k_{il} = \begin{cases} \gamma * Q / d_{ij} (1 - \dfrac{d_{il} * (d_{il})^w}{\overline{d}^{w+1}} \mathrm{ctg}\theta) & \text{if } d_{il} < \overline{d}^{w+1} / (d_{ij})^w * \mathrm{tg}\theta \\ 0 & \text{otherwise} \end{cases} \tag{6.36}$$

$$D^k_{jl} = \begin{cases} \gamma * Q / d_{ij} (1 - \dfrac{d_{jl} * (d_{jl})^w}{\overline{d}^{w+1}} \mathrm{ctg}\theta) & \text{if } d_{jl} < \overline{d}^{w+1} / (d_{ij})^w * \mathrm{tg}\theta \\ 0 & \text{otherwise} \end{cases} \tag{6.37}$$

式（6.33）表示第 k 只蚂蚁在时刻 t 到 t+1 之间经过路径 ij，式（6.34）表示第 k 只蚂蚁在时刻 t 到 t+1 之间经过城市 i 但不经过城市 l，式（6.35）表示第 k 只蚂蚁在时刻 t 到 t+1 之间经过城市 j 但不经过城市 l。即在基本的蚁群模型中，每只蚂蚁每走一步只改变其刚好经过的那段路径上的信息素的浓度，但在信息素扩散的蚁群算法模型中，该蚂蚁可能会改变多条路径上的信息素的浓度。这将大大提高蚂蚁群体之间的合作效果，增强蚁群算法的有效性。在式（6.36）和式（6.37）的计算过程中，取 $h = \overline{d}^{w+1} / (d_{ij})^w$，$w$ 为大于 1 的可调常数，d 为各城

市的平均距离。假定 $D_{\max}=\gamma*\Delta\tau_{ij}^{k}$，其中 γ 是小于 1 的可调常数。

通过实验观察，采用该算法在整个进化过程中，解的多样性一直很好，因此具有不断获得新的最优解的能力，使得该算法可以获得全局最优解，而不易陷入局部最优解。

3．混合蚁群算法[42]

所谓混合蚁群算法主要是针对混合生产调度问题而提出的一种蚁群算法。混合生产调度是一类具有高度复杂性的生产调度问题。这类问题包含两个性质不同的部分：连续时间过程和离散时间过程。根据这两个部分，混合蚁群算法采用如下调度策略。

（1）针对混合调度问题解空间中存在不同类型的待优化变量，采用了不同的搜索图生成方法。

（2）根据优化变量在逻辑上的不同层次，采用嵌套的蚁群搜索方法，在不同层次分别进行不同搜索图上的搜索。

通过仿真研究表明，嵌套混合蚁群算法在求解特定混合生产调度问题中，解的有效性和平稳性有明显提高。

6.2.3 蚁群算法的应用

对蚂蚁行为的研究已导致各种相关算法的开发，并把它们应用于求解各种问题中，这些算法建立了蚂蚁搜索行为的模型，产生了新的组合优化算法，应用于网络路径选择和作业调度等方面。蚂蚁动态地分配劳动力产生出自适应任务分配策略，它们合作搬运的特性产生了机器人式的实现。把蚁群算法进行优化的工作称为蚁群优化，它已在解决组合优化问题中显示出优越性。

蚁群算法和蚁群优化已被成功地应用于二次分配问题（Quadratic Assignment Problem，QAP）、作业调度问题（Job-Scheduling Problem，JSP）、图表着色问题（Graph Coloring Problem，GCP）、电话网络和数据通信网络的路由优化以及机器人建模和优化等。另外，蚁群算法还可以应用到数据挖掘中，实现分类及聚类的任务。下面详细介绍一下基于蚁群算法的分类规则挖掘和聚类分析。

1．基于蚁群算法的分类规则挖掘[43,44]

分类在数据挖掘中是一项非常重要的任务，目前在商业上应用最多。分类的目的是产生一个分类函数或分类模型，该模型能把数据库中的数据项映射到给定类别中的某一个上。在数据挖掘中，一般采用的分类算法有决策树、神经网络、径向基函数（Radial Basis Functions）等。

分类算法产生的规则一般采用产生式规则的方式来表示，即 IF-THEN，例如：

IF　<condition>　THEN　<class>

IF 部分为规则前件，THEN 部分为规则后件。通常规则前件是属性值对的逻辑与。Ant-Miner 算法就是一种基于蚁群的分类规则提取算法，该算法采用蚂蚁在数据库的属性空间中随机搜索逐步形成相对应规则的前件。

算法的输入是一个空的规则列表和一个包含所有训练样本的训练集合。蚂蚁个体按照规则构造原则、启发函数及规则的剪枝算法生成相应的规则，并把该规则加入到规则列表中，同时从训练样本集合中删除包含在该规则中的训练样本。重复执行该过程，直到没有包含在规则中的训练样本的数量小于用户设定的阈值。

在整个算法中，起决定作用的有以下两个方面。

第一是蚂蚁选择属性值对的策略。当前的某个蚂蚁，从空规则开始，每一次都重复地增加一个属性值对到一个不完整的规则中，其选择策略定义如下：

$$P_{ij}=\frac{\eta_{ij}*\varphi_{ij}(t)}{\sum_{i=1}^{a}x_i*\sum_{j=1}^{b_i}(\eta_{ij}*\varphi_{ij}(t))} \tag{6.38}$$

其中，η_{ij} 是启发函数，它标示了第 i 个属性的第 j 个取值对于分类的重要程度。它越高，该属性值对被加到规则中的概率也就越大；$\varphi_{ij}(t)$ 是在第 t 次重复时，第 i 个属性的第 j 个取值的信息素的浓度；a 是属性个数；x_i 表示第 i 个属性是否被当前的蚂蚁选择，如果没有被选择取 1，反之取 0；b_i 表示第 i 个属性的所有属性值。

第二是启发函数。该算法的启发函数是基于信息理论的，通过每个属性值的信息熵来度量其在规则中的重要性。其定义如下：

$$\eta_{ij}=\frac{\log_2 k-H(W\mid A_i=V_{ij})}{\sum_{i=1}^{a}x_i*\sum_{j=1}^{b_i}(\log_2 k-H(W\mid A_i=V_{ij}))} \tag{6.39}$$

另外的如规则的剪枝、信息素的更新及规则质量的评价等，就不赘述了。该算法与典型的分类算法 CN2 相比，准确性与 CN2 相当，且发现的规则列表比 CN2 获得的规则列表简单。

2．基于蚁群算法的聚类分析[45]

基于蚁群算法的聚类分析具有群体智能算法的共同特点，它利用个体与个体和个体与环境的交互作用，不必预设聚类中心的数目，实现自组织聚类过程，具有健壮性、可视化等特点。基于蚁群算法的聚类分析的主要思路是将待聚类的对象随机放置在一个两维网格的环境中，每一个对象有一个随机初始位置，每一只蚂蚁能够在网格上移动，并测量当前对象在局部环境的群体相似度，通过概率转换函数将群体相似度转换成移动对象的概率，以这个概率拾起或放下对象。蚁群联合行动导致属于同一类别的对象在同一个空间区域能聚集在一起。

群体相似度是一个待聚类模式（对象）与其所在的局部环境中所有其他模式的综合相似度。群体相似度的基本测量公式是：

$$f(o_i)=\sum_{o_j\in \mathrm{Neigh}(v)}\left[1-\frac{d(o_i,o_j)}{\alpha}\right] \tag{6.40}$$

其中，Neigh (*r*)表示局部环境，在两维网格环境中通常表示以 *r* 为半径的圆形区域。$d(o_i,o_j)$ 表示对象属性空间里的对象 o_i 与 o_j 之间的距离，常用方法是欧氏距离和余弦距离等。α 定义为群体相似系数。它是群体相似度测量的关键系数，它直接影响聚类中心的个数，同时也影响聚类分析的收敛速度。概率转换函数是将群体相似度转换为简单个体移动待聚类模式（对象）概率的函数。它是以群体相似度为变量的函数，此函数的值域是[0,1]。同时概率转换函数也可称为概率转换曲线。它通常是两条相对的曲线，分别对应模式拾起转换概率 P_p 和模式放下转换概率 P_d。概率转换函数制定的主要原则是群体相似度越大，模式拾起转换概率越小，群体相似度越小，模式拾起转换概率越大，而模式放下转换概率遵循大致相反的规律。

依照概率转换函数制定的主要原则，基于蚁群算法的聚类分析将模式拾起转换概率 P_p 和模式放下转换概率 P_d 定义为以 *k* 为斜率的直线，如下所示：

$$P_p=\begin{cases}1-\varepsilon & f(o_i)\leqslant 0\\ 1-k*f(o_i) & 0<f(o_i)\leqslant 1/k\\ 0 & f(o_i)>1/k\end{cases} \tag{6.41}$$

$$P_d=\begin{cases}1-\varepsilon & f(o_i)\geqslant 1/k\\ k*f(o_i) & 0<f(o_i)<1/k\\ 0 & f(o_i)\leqslant 0\end{cases} \tag{6.42}$$

其中，ε 是一个较小的正小数，它的作用是便于算法的收敛。

蚁群算法是一个十分年轻的研究领域，刚刚走过十几年的路程，尚未形成完整的理论体系，其参数选择更多地依赖试验和经验，许多实际问题也有待深入研究与解决。随着蚁群算法的深入开展，它将会提供一个分布式和网络化的优化算法，从而促进计算智能的进一步发展。

6.3 小结

群体智能作为一种新兴演化计算技术，已成为新的研究热点，已完成的理论和应用研究证明群体智能方法是一种能够有效解决大多数全局优化问题的新方法。目前，群体智能理论

研究领域有两种主要的算法：粒子群优化算法和蚁群算法。

粒子群优化算法是一种基于群体搜索的算法，它建立在模拟鸟群社会的基础上。粒子群优化算法通过粒子自身的速度、认知和社会部分这些心理学假设，体现了粒子在寻求一致认知过程中，个体往往记住它们的信念，同时考虑同事的信念。当个体察觉同事信念较好的时候，它将进行适应性的调整。由此可见，粒子群优化算法是一种共生合作算法。建立这种社会行为模型的结果是：在搜索过程中，粒子随机地回到搜索空间中一个原先成功的区域。 为了进一步提高粒子群优化算法的寻优能力，研究者们从参数设置、粒子多样性、种群结构和算法融合方面对其进行了改进。

蚁群算法是从生物进化和仿生学角度出发，通过研究蚂蚁寻找路径的自然行为提出来的。并用该方法求解 TSP 问题、二次分配问题和作业调动问题，取得了较好的结果。作为一种随机优化方法，蚁群算法不需要任何先验知识，最初只是随机地选择搜索路径，随着对解空间的“了解”，搜索变得有规律，并逐渐逼近直至最终达到全局最优解。蚁群算法对搜索空间的“了解”机制主要包括：蚂蚁的记忆、信息素的传播及蚂蚁的集群活动。虽然蚁群算法具有鲁棒性强、能够进行分布计算和易于与其他方法结合等优点，但是该算法需要较长的计算时间，容易出现停滞现象。因此研究者们提出了一些改进的算法，如具有随机扰动特征的蚁群算法、基于信息素扩散的蚁群算法等。

参 考 文 献

[1] 彭喜元，彭宇，戴毓丰．群智能理论及应用．电子学报，2003,32(12A)：1982-1988.

[2] Kennedy J, Eberhart R C. Particle Swarm Optimization. Proc IEEE International Conference on Neural Networkss, IV. Piscataway, NJ: IEEE Service Center 1995:1942-1948.

[3] James Kennedy, Russell C Eberhart. Swarm Intelligence.San Francisco:Morgan Kaufmann Publisher,2001:165-178.

[4] Shi Y, Eberhart R C. A modified particle swarm optimizer. Proceedings of IEEE International Conference on Evolutionary Computation, Anchorage,1998:69-73.

[5] 纪震，廖惠连，吴青华．粒子群算法及应用．北京：科学出版社，2009.

[6] Kennedy J, Eberhart R C. A discrete binary version of the particle swarm algorithm. IEEE Press,1997:4104-4108.

[7] 杨维，李歧强．粒子群优化算法综述．中国工程科学，2004,6(5)：87-94.

[8] Shi Y, Eberhart R C. Fuzzy adaptive particle swarm optimization. Proceedings of the

Congress on Evolutionary Computation. Seoul, Korea,2001.

[9] van den Bergh F. An analysis of particle swarm optimizers. South Africa:Department of Computer Science, University of Pretoria,2002.

[10] Clerc M. The Swarm and Queen: Towards a Deterministic and Adaptive particle Swarm Optimization. Proc. IEEE International Congress on Evolutionary Computation(CEC 1999), Vol.3:1951-1957.

[11] Clerc M, Kennedy J. The particle swarm-explosion, stability, and convergence in a multidimensional complex space . IEEE Trans. On Evolutionary Computation, 2002,6(1): 58-73.

[12] 方俊．粒子群算法及其应用研究．电子科技大学硕士论文，2006.

[13] Trelea I C. The particle swarm optimization algorithm: convergence analysis and parameter selection[J]. Information Processing Letters,2003,85(6):317-325.

[14] El-Gallad A ,El-Hawary M,Sallam A ,Kalas A. Enhancing the particle swarm optimizer via proper parameters selection . IEEE CCECE02 Proceedings. Piscataway ,NJ ,Canadian : IEEE service center ,2002:792 - 797.

[15] J E Fieldsend ,S Singh. On the selection of gbest ,lbest ,and pbest individuals ,the use of turbulence and the impact of inertia in multiobjective PSO. http :// citeseer. nj . nec. com /fieldsend02selection. html.

[16] Jacques Riget ,Jakob S Vesterstrom. A diversity-guided particle swarm optimization the ARPSO . http :/ / citeseer. nj . nec. com.

[17] Lovbjerg M, Krink T. Extending particle swarms with self-organizedcriticality. Proceedings of the Fourth Congress on evolutionary computation (CEC22002) . Honolulu , HI USA ,2002: 1588 -1593.

[18] T. Krink, J.S. Vesterstrom, J. Riget. Particle Swarm Optimisation with Spatial Particle Extension. Evolutionary Computation, 2002. CEC '02. Proceedings of the 2002 Congress on:1474-1479.

[19] Brists R, Engelbrchta P, Bergh F D. A niching particle swarm optimizer. Proceedings Conf. on Simulated Evolution and Learming, Singapore, IEEE Inc.,2002:1037-1040.

[20] 贾东立，张家树．基于混沌变异的小生境粒子群算法．控制与决策，2007,22(1)：117-120.

[21] Lee C G, Cho D H, Jung H K. Niche genetic algorithm with restricted competition selection for multimodal function optimization . IEEE Trans on Magnetics,1999, 35(3):1122-1125.

[22] 刘健辰，沈洪远，姚屏，刘晓莉．一种基于聚类分析的小生境微粒群优化算法．湖南科技大学学报（自然科学版），2006,21(3)：73-76.
[23] Angeline P J. Using selection to improve particle swarm optimization . IEEE International Conference on Evolutionary Computation, Anchorage,1998:84-89.
[24] Lovjerg M, Rasmussen T K, Krink T. Hybrid particle swarm optimizer with breeding and subpopulation .Proceedings of the Third Genetic and Evolutionary Computation Conference(GECCO-2001), 2001:607-614.
[25] 王东升，曹磊．混沌、分形及其应用．合肥：中国科学技术大学出版社，1995.
[26] 高鹰，谢胜利．混沌粒子群优化算法．计算机科学，2004,31(8)：13-15.
[27] 高尚，杨静宇．混沌粒子群优化算法研究．模式识别与人工智能．2006, 19(2)：66-70.
[28] 陈如清，俞金寿．混沌粒子群混合优化算法的研究与应用．系统仿真学报．2008, 20(3)：685-688.
[29] 尤勇，王孙安，盛万兴．新型混沌优化方法的研究及应用．西安交通大学学报，2003,37(1)：69-72.
[30] S.Kirkpatrick, C.D.Jr.Gelatt, M.P.Vecchi. Optimization by simulated annealing[J]. Science, 1983,220:671-680.
[31] 高鹰，谢胜利．基于模拟退火的粒子群优化算法[J]．计算机工程与应用，2004：47-50.
[32] 黄岚，王康平，周春光，庞巍，董龙江，彭利．粒子群优化算法求解旅行商问题[J]．吉林大学学报（理学版），2003,41(8)：477-480.
[33] 高海兵，高亮，周驰，喻道远．基于粒子群优化的神经网络训练算法研究[J]．电子学报，2004,32(9)：1572-1574.
[34] 段晓东，王存睿，王楠楠，刘向东，石丽．一种基于粒子群算法的分类器设计[J]．计算机工程，2005,31(20)：107-109.
[35] 高尚，杨静宇．一种新的基于粒子群算法的聚类方法[J]．南京航空航天大学学报，2006,38 增(7)：62-65.
[36] 李宁，付国江，库少平，陈明俊．粒子群优化算法的发展与展望[J]．武汉理工大学学报・信息与管理工程版，2005,27(2)：26-29.
[37] M Dorigo,V Maniezzo, A Colorni. Distributed optimization by ant colonies[A]. Proc 1st European conf Artificial Life[C]. Pans, France:Elsevier,1991:134-142.
[38] 蔡自兴，徐光佑．人工智能及其应用[M]．北京：清华大学出版社，2004.
[39] 王剑，李平，杨春节．蚁群算法的理论与应用[J]．机电工程，2003,20 (5)：126-129.
[40] 郝晋，石立宝，周家启．具有随机扰动特性的蚁群算法[J]．仪器仪表学报，2001,22 (增 4)：350-352.

[41] 黄国锐，曹先彬，王煦法．基于信息素扩散的蚁群算法[J]．电子学报，2004,32 (5)：866-868.
[42] 李艳君．拟生态系统算法及其在工业过程控制中的应用[D]．杭州：浙江大学，2001.
[43] 吴正龙，王儒敬，滕明贵，许梅生．基于蚁群算法的分类规则挖掘算法[J]．计算机工程与应用，2004(20)：30-33.
[44] Rafael S, Parpinelli, Heitor S.Data Mining With an Ant Colony Optimization Algorithm[J].IEEE TRANSACTIONS ON EVOLUTIONARY COMPUTING, 2002,6(4):321-332.
[45] 吴斌，傅伟鹏，郑毅，刘少辉，史忠植．一种基于群体智能的 Web 文档聚类算法[J]．计算机研究与发展，2002,39(11)：1430-1435.

Chapter 7

第7章 人工免疫

免疫是生物体的特异性生理反应，由具有免疫功能的器官、组织、细胞、免疫效应分子及基因等组成。免疫系统通过分布在全身的不同种类的淋巴细胞识别和清除侵入生物体的抗原性异物。当生物系统受到外界病毒侵害时，便激活自身的免疫系统，其目标是尽可能保证整个生物系统的基本生理功能得到正常运转。从计算的角度来看，生物免疫系统是一个高度并行、分布、自适应和自组织的系统，具有很强的学习、识别、记忆和特征提取能力[1]。人们自然希望从生物免疫系统的运行机制中获取灵感，开发面向应用的免疫系统计算模型——人工免疫系统（Artificial Immune System，AIS），用于解决工程实际问题。

人工免疫系统通过学习外界物质的自然防御机理的学习技术，提供噪声忍耐、无教师学习、自组织、记忆等进化学习机理，结合了分类器、神经网络和机器推理等系统的一些优点，因此具有提供新颖的解决问题的潜力。其研究成果涉及控制、数据处理、优化学习和故障诊断等领域。目前 AIS 已发展成为计算智能研究的一个崭新的分支。

7.1 AIS 的生物原型和免疫机理

7.1.1 AIS 的生物原型[1~3]

AIS 的生物原型是指人体等高等脊椎动物的免疫系统（在不引起混淆的情况下，下面将

其简称为免疫系统）。

免疫系统抵御外部入侵，使其机体免受病原侵害的应答反应称为免疫（Immunity）。外部有害病原入侵机体并激活免疫细胞，诱导其发生反应的过程称为免疫应答。免疫应答分为固有性免疫和获得性免疫两种，前者为机体先天获得，可对病原进行快速清除；后者进行特异性识别并清除病原体，具有特异性、记忆、区分自我与非我、多样性和自我调节等优良特性。诱导免疫系统产生免疫应答的物质称为抗原，能与抗原进行特异性结合的免疫细胞称为抗体。

免疫系统的主要功能是识别体内细胞，将其归类为“自我”和“非我”，并引发适当的防卫机制去除“非我”。自我对应于机体自身的组织；非我对应于外来有害病原或体内病变组织。免疫应答主要由分布在生物体全身的免疫细胞来实现。免疫细胞泛指所有参与免疫应答过程的相关细胞，包括吞噬细胞、NK 细胞、淋巴细胞等。淋巴细胞又分为 B 细胞和 T 细胞两种。B 细胞的主要功能是产生抗体，且每个 B 细胞只产生一种抗体。免疫系统主要依靠抗体来对入侵抗原进行攻击以保护有机体。T 细胞的主要功能是调节其他细胞的活动或直接对抗原实施攻击。成熟的 B 细胞产生于骨髓中，成熟的 T 细胞产生于胸腺之中。B 细胞和 T 细胞成熟之后进行克隆增殖、分化并表达功能。两种淋巴细胞共同作用并相互影响和控制对方功能，形成了机体内部高度规律的反馈型免疫网络。

7.1.2 AIS 的免疫机理

从信息处理的角度来看，免疫系统具备强大的识别、学习和记忆的能力，以及分布式、自组织和多样性特性，这些显著的特性不断地吸引着研究人员从免疫系统中抽取有用的隐喻机制，开发相应的 AIS 模型和算法用于信息处理和问题求解。图 7.1 给出了 AIS 免疫机理的主要内容描述。

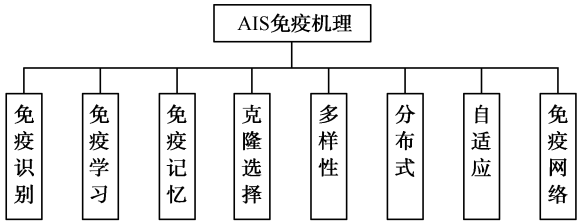


图 7.1 AIS 免疫机理

对于在工程应用中可借鉴的相关机理扼要阐述如下。

1．免疫记忆

免疫系统的记忆作用是众所周知的，如患了一次麻疹后，第二次感染了同样的病毒也不致发病，这是因为在一次免疫响应后，如果同类抗原再刺激，在短时间内，免疫系统会产生比上一次多得多的抗体，同时与该抗原的亲和力也提高了[4]。免疫记忆属于联想式记忆，是AIS 区别于其他进化算法的重要特性之一。Farmer[5]首先指出免疫记忆可以看做一种联想式记忆（Associative Memory）模型。Smith[6]对免疫记忆模型与稀疏分布记忆（Sparse Distributed Memory，SDM）模型进行了对比，指出初次免疫应答对应着 SDM 向记忆中存储信息的过程，而再次和交叉免疫应答则可以看做是 SDM 读取记忆信息的过程。总之，免疫记忆是提高算法执行效率的一种非常有效的手段。

2．克隆选择

由于遗传和免疫细胞在增殖中的基因突变，形成了免疫细胞的多样性，这些细胞的不断增殖形成无性繁殖系。细胞的无性繁殖称为克隆。克隆选择原理最先由 Jerne[7]提出，后由 Burnet[8]予以完整阐述。它的主要特征是免疫细胞在抗原刺激下产生克隆增殖，随后通过遗传变异分化为多样性效应细胞（如抗体细胞）和记忆细胞。克隆选择对应着一个亲和度成熟（Affinity Maturation）的过程，即对抗原亲和度较低的个体在克隆选择机制的作用下，经历增殖复制和变异操作后，其亲和度逐步提高而“成熟”的过程。因此亲和度成熟本质上是一个达尔文式的选择和变异的过程，克隆选择原理是通过采用交叉、变异等遗传算子和相应的群体控制机制实现的。

根据克隆选择原理，De Castro[9]提出了克隆选择算法模型，并在模式识别、组合优化和多峰值函数优化中得到了验证。Kim[10,11]将克隆选择原理用于网络入侵检测。其算法的核心在于增殖复制算子和变异算子，前者与个体亲和度成正比，保证群体亲和度逐步增大；后者与个体的亲和度成反比，保留最佳个体并改进较差个体。

3．多样性机理

根据免疫学知识，免疫系统大约含有 10^6 种不同的蛋白质，但外部潜在的抗原或待识别的模式种类有 10^{16} 之多。要实现对数量级远远大于自身的抗原识别，需要有效的多样性个体产生机制。抗体多样性的生物机制主要包括免疫受体库的组合式重整、体细胞高突变及基因转换等，而目前比较公认的多样性产生机制是抗原受体库的基因片段重组方法，其中基因片段是抗体的组成单位之一。

多样性免疫机理可以广泛应用于优化搜索过程，特别是组合优化与多峰函数优化。它不尝试于全局优化，而是进化地处理不同抗原的抗体，从而提高全局搜索能力，避免陷入局部

最优。将该多样性机理用于遗传算法中，可以有效地改善算法的局部收敛性能。另外，多样性产生机制可为需要多样性数据集合的研究与应用提供借鉴，如神经网络集成等[12]。

4．其他机理

免疫系统所具有的无中心控制的分布自治机理、自组织存储机理、免疫网络及非线性机理等均可用于建立人工免疫系统。

7.2 AIS 的模型及算法

基于免疫系统的免疫机理开发的 AIS 模型主要有人工免疫网络模型和 AIS 应用框架模型，其实现算法主要有反向选择算法、基于 GA 算子的免疫算法、克隆选择算法、免疫学习算法等。

7.2.1 AIS 的模型

由于免疫系统本身比较复杂，因此人工免疫系统模型的研究相对较少。主要包括人工免疫网络模型和 AIS 应用框架模型。

1．人工免疫网络模型

人工免疫网络模型将 AIS 视为一个由节点（淋巴细胞）组成的网络结构，通过节点之间的信息传递和相互作用达到识别、效应、记忆等免疫系统功能，主要有独特型网络模型、互联耦合网络模型、多值网络模型、抗体网络模型等。

N.K.Jerne[13]根据现代免疫学对抗体分子独特型的认识，在克隆选择学说的基础上提出了著名的独特型网络学说（Idiotypic Networks Theory），即免疫网络模型，以阐明免疫系统内部对免疫应答的自我调节。已有的资料表明，研究免疫系统的网络对免疫系统的发生、内在关系等方面都有重要意义。独特型网络模型已在机器人和控制工程等领域获得了成功应用。

Ishiguro[14]提出了一种互联耦合人工免疫网络模型，即免疫系统是通过多个完成某一特定任务的局部免疫网络之间的相互通信来形成大规模免疫网络。该模型已用于机器人的行走控制和路径规划之中。Tang[15]提出了一种多值免疫网络模型，通过字符识别显示出多值免疫网络在记忆模式、记忆容量方面，特别是在噪声免疫能力方面要优于二进制网络模型。

在免疫系统内部存在一个抗体之间相互作用的网络。De Castro[3]据此提出了一个抗体网络模型 ABNET，该模型以克隆选择原理为基础，其核心为网络的生成算法，生成的抗体网络

用于识别给定数量的抗原。ABNET 的主要特征为竞争式学习、网络结构的自动生成和连接强度（权重）的二进制表示等。从机器学习的角度来看，它是一种性能优异的无监督学习策略。

2．AIS 应用框架模型

随着 AIS 探讨的深入，研究人员致力于开发统一的 AIS 应用框架模型。下面详细介绍 ARTIS[16]模型，该模型已成功应用于网络入侵检测中。

免疫系统中自我和非我的识别是基于蛋白质链之间的化学绑定的。在 ARTIS 中使用了固定长度为 L 的二进制字符串来表示蛋白质链，长度为 L 的所有字符串集合形成了一个论域 U，而 U 被划分为两个不相交的子集，分别称做自我集合 S 和非我集合 N，即 $U=S\cup N$，$S\cap N=\phi$。随后使用一个图 $G=(V,E)$ 来对检测器所处的分布式环境进行建模，其中 V 包含一个检测器的局部集合，而检测器可以在图上沿着边 E 来遍历节点。检测器的识别采用部分匹配方法，并由协同刺激信号进行激活。检测器由隐性选择算法训练，在一定生命周期执行检测任务。另外，Forrest 提出了基于记忆的检测模式，通过记忆机制加速对异常特征的识别。该应用框架模型较为完整地给出了从免疫系统到 AIS 的模型映射，提供了一个完整的 AIS 问题求解范式。

7.2.2　AIS 的算法

免疫算法的设计有两种思路：一种基于白箱模拟的方法，重点在于结构和机理上的模拟，免疫算法的设计依赖于生物免疫系统的知识；另一种基于黑箱模拟的方法，重点在于输入/输出和功能上的模拟[17]。

1．白箱模拟法

现在很难做到从结构和机理上完全模拟生物免疫机制，因为人类还没有完全解开生物免疫之谜，还有许多问题需要进一步研究。因而，目前不少研究者往往按照白箱模拟法的思路，借用生物免疫机制的一些概念，从形式上进行一定的模拟，以实现对系统人工免疫的目的。例如，有的算法模拟生命科学中的免疫理论，引入了免疫算子来改进遗传算法。免疫算子根据生物免疫理论分为全免疫和目标免疫两种类型，分别对应于生命科学的非特异性免疫和特异性免疫。

2．黑箱模拟法

黑箱模拟法间接地从输入/输出的特征来考查人工系统对自然系统的模拟。免疫算法常采用遗传算法或进化算法对外界攻击或病毒进行学习，产生与外界攻击或病毒相克的抗体。所

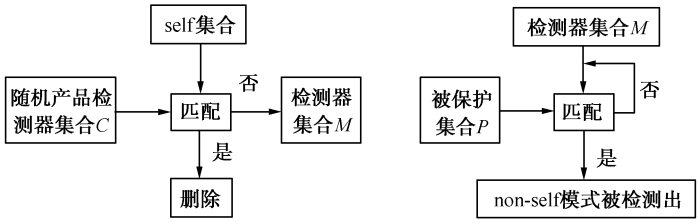
以，免疫算法一般采用遗传学习机制。下面重点介绍几种人工免疫算法。

1）反向选择算法

S.Forrest 等人[18]在 1994 年提出了反向选择算法（Negative-selection Algorithm），原理是免疫系统可以区分自身和非自身细胞。当给定一个特定问题时，反向选择算法可以具体描述为两个部分[19]。

（1）产生检测器集合，如图 7.2（a）所示。使用相同的表达式随机产生候选检测器集合 *C*；比较 *C* 中的元素与 self 集合中的元素。如果匹配，则从 *C* 中删除该元素；否则，将此元素存储在检测器集合 *M* 中。

（2）监测 non-self 模式的出现，如图 7.2（b）所示。假设要保护的集合是 *P*（*P* 中有可能包含除 self 外的新模式），若 *P* 中的某个元素与检测器集合中一个检测器匹配，说明该元素是 non-self，将其从 *P* 中删除。



（a）产生检测器集合　　（b）监测non-self模式的出现

图 7.2　反向选择算法

在反向选择算法中，常见的检测器生成算法有穷举（Exhaustive）、线性（Linear）、贪婪（Greedy）、二元模板（Binary Template）、NSMutation 等几种算法。而常用的匹配算法有 *r* 位连续（*r*-contiguous）、*r* 块（*r*-chunk）、海明距离及其变种 R&T 匹配（Roger 和 Tanimoto）等。

反向选择算法和检测器生成算法的不同表示方法正在研究中。正在研究的表示方法包括 Hyper-Rect-Angles（超矩形），模糊规则和 Hyper-Spheres（超球体）。目前提出的四类不同检测器生成算法包括带有检测规则的反向选择（NSDR）、带有模糊检测规则的反向选择（NSFDR）、真值评价反向选择（RNS）和随机化真值评价反向选择（RRNS）。同时发展的还有一种结合了 RNS 与分类算法的混合免疫学习算法。

反向选择算法的一个主要优点就是对异常模式（非自身）不需要有先验知识，可以对未知入侵模式进行有效的防御，但同时也带来了一些问题：在 Forrest 最初描述这个算法时，为了可以对绝大多数入侵进行反应，使用了概率分析的方法估计检测器的有效数量，为达到一定的可靠性，对应的检测器集合十分庞大，系统初始化十分困难；另外，为了选择有效检测器，计算量随自身集合的扩大呈指数增长。针对这些问题，尽管 Helman 和 Forrest 于 1994 年

提出了一种更有效的检测器生成算法，但问题仍未被完全解决。

2）基于 GA 算子的免疫算法[1]

这类免疫算法采用类似遗传算法的搜索策略，借用了遗传算法的选择、交叉和变异算子（有的只有变异算子），但在群体搜索策略、解的表示和记忆单元设置等方面与遗传算法有所不同。从搜索策略来讲，遗传算法采用适应度函数来指导搜索过程，AIS 采用亲和度（如 Hamming、信息熵等）进行度量；遗传算法采用二进制数或浮点字符来表示一个完整的解，而 AIS 大多采用部分编码，其个体编码只对应于解的一部分；另外，AIS 与 GA 的群体控制策略也有所不同，GA 无明显的记忆单元，而 AIS 则保存最优个体记忆信息，用于加速局部搜索或抑制早熟收敛，从而使算法快速收敛到全局最优解。采用 GA 算子的免疫算法目前尚无统一框架，但已经在求解诸如组合优化等问题中显示了强大的优化搜索能力。

3）克隆选择算法

基于克隆选择原理，De Castro[9]提出了一种克隆选择算法，核心是比例复制和比例变异算子，在解决诸如模式识别等复杂机器学习任务方面，该算法有显著能力。算法流程如下。

Step1：产生候选方案的集合 $S(P)$，该集合为记忆细胞子集 (M) 和剩余群体 (P_r) 的总和 $(P = P_r + M)$。

Step2：基于亲和度度量确定群体 P 中的 n 个最佳个体 P_n。

Step3：对群体中的这 n 个最佳个体进行克隆（复制），生成临时克隆群体 C。克隆规模是抗原亲和度度量的单调递增函数。

Step4：对克隆生成的群体施加变异操作，变异概率反比于抗体的亲和度，从而生成一个成熟的抗体群体 (C^*)。

Step5：从 (C^*) 中重新选择改进个体组成记忆集合，P 集合的一些成员可以由 (C^*) 的其他改进成员加以替换。

Step6：将群体中的 d 个低亲和度的抗体予以替换，从而维持抗体的多样性。

该算法成功应用到了二进制字符识别、多峰函数优化和组合优化中，取得了良好效果。对比遗传算法，克隆选择算法在编码机制和评价函数的构造上与其基本一致，但搜索的策略和步骤有所不同；而且通过免疫记忆机制，该算法可以保存各个局部最优解，这对于多峰函数优化十分重要。

4）免疫网络算法

免疫网络算法是基于免疫网络模型提出来的。De Castro 和 Timmis 分别于 2000 年和 2001 年从计算机科学的角度提出了免疫网络算法[20,21]。这两种算法在很大程度上是一致的。Timmis 在免疫网络的一种扩展模型 AINE 中加入了人工识别球（Artificial Recognition Ball，ARB）的概念。这种想法来源于免疫学中的识别球，即在抗体周围的一定范围内抗原都能被识别。ARB 用来表示大量相似的 B 细胞。在数学模型上，ARB 代表的是一个能够与其他 ARB，或者 B

细胞在欧氏距离上匹配的 n 维数据对象。当两个 ARB 之间的相似性低于网络相似性阈值时，两个 B 细胞之间将会建立一个连接。基于 ARB 的概念，陆续出现了资源受限人工免疫系统 RLAIS（Resource Limited AIS）和自稳定人工免疫系统 SSAIS（Self-Stabilizing AIS）。RLAIS 通过预先定义 ARB 中 B 细胞的数目来达到种群控制的目的，即整个网络是资源有限的。而 SSAIS 模型中分配给 ARB 的资源并不固定，资源的配置由 ARB 来处理。

5）免疫学习算法

机器学习是系统内部的适应性变化，该变化使得系统此后执行同一问题范围内的相似任务时效率更高。从该定义我们不难看出这与 AIS 的免疫学习机理十分吻合。Farmer[5]首先对免疫系统的学习特性进行了探索性研究，指出其与 Holland 的分类器系统具有相似性。随后 Hunt[22]基于免疫网络理论给出了一种有监督的机器学习算法。Ishida[23]提出了一种基于 PDP 模型的 AIS 学习算法，并将其应用到故障诊断中。

7.3 人工免疫系统的应用

近年来，基于免疫系统原理开发的各种模型和算法广泛地应用在科学研究和工程实践中，下面对典型的应用领域进行简要的介绍。

1．信息安全

信息的安全性主要取决于以下三个方面：检测计算机设备的非授权使用情况、维护数据文件的完整性和防止计算机病毒扩散。而安全策略的核心问题是对于非法入侵的检测，可将其理解为识别自我和非我的问题。鉴于免疫系统具有保护机体的强大能力，相应的 AIS 模型在信息安全方面得到了广泛应用。Forrest 及其研究小组最早开展了基于 AIS 的信息安全研究并提出了计算机免疫学的概念，致力于建立自适应的计算机与网络免疫系统，从而增强现行的计算机与网络系统的安全性[24]。

2．模式识别

免疫系统强大的识别能力在模式识别方面得到了广泛的应用，主要涉及了反向选择、克隆选择和免疫网络等免疫机理。Forrest[16]给出了免疫系统的二进制模型，研究了模式识别问题和免疫系统中个体与群体水平上的学习机制，其中抗体和抗原用简单的二进制编码表示，模式匹配采用部分匹配规则。Dasgupta[25]研究了光谱识别问题，采用二进制对光谱识别的对象进行了具体描述，同时还给出了相应的匹配函数及识别算法。De Castro[9]研究了基于克隆选择机理的字符识别问题，采用状态空间表示待识别的模式。

3．数据挖掘

数据挖掘是“从巨量数据中获取有效的、新颖的、潜在有用的、最终可理解模式的非平凡过程”。采用 AIS 模型的数据挖掘目前主要集中在数据聚类分析、数据浓缩、归类任务等方面。Hunt 和 Cooke[22]研究了基于 AIS 模型的无监督学习算法，将其用到了 DNA 序列的分类任务中。在对 AIS 与聚类分析（Cluster Analysis）、科赫网络（Kohone Network）进行对比分析后，Timmis 指出 AIS 在数据分析中的应用是可行且有效的[26]。他构造了一种与领域无关的无监督机器学习方法用于实验数据的聚类分析，并进一步给出了用于数据分析的有限资源 AIS 模型 RLAIS[21]，该模型在多谱影像的深入数据分析和网络故障预测中得到了应用。

4．智能优化

作为一种智能优化搜索策略，AIS 在函数优化、组合优化、调度问题等方面得到应用并取得了很好的效果。组合优化是运筹学的一个重要分支，它主要通过数学方法去寻找离散事件的最优编排、分组、次序或筛选等。随着这类问题规模的扩大，其问题空间呈现组合爆炸特性，难以用常规优化方法求解。

基于免疫原理实现的免疫算法在组合优化求解中显示出了强大的能力，这些问题包括旅行商问题（TSP）[27]、二次分配问题（QAP）[28]、装箱问题[29]、调度问题[30]等。在大多数情况下，免疫算法取得了比现有启发式算法更好的求解结果，尤其在求解的效率方面，显示出 AIS 在智能优化领域具有广阔的应用前景。

5．机器人学

机器人学是目前人工智能领域的一个研究热点，涉及的研究领域非常广。借鉴 AIS 的学习、识别、分布式和自适应等仿生机理，AIS 在机器人行为控制、行为仲裁和路径规划等方面得到了很好的应用。Mitsumoto[31]基于免疫系统的“自我—非我”识别网络，开发了动态环境中的自适应移动测量算法并将其应用到多主体机器人系统中，他还进一步研究了基于免疫的自组织多机器人系统群体控制策略。

7.4　小结

人工免疫系统是从生物免疫系统的运行机制中获取灵感，开发出的面向应用的免疫系统计算模型。它具有免疫记忆、克隆选择、多样性，以及分布自治、自组织存储、免疫网络非线性等机理。目前，人工免疫模型主要有人工免疫网络模型和人工免疫应用框架模型，其实

现算法主要有反向选择算法、基于 GA 算子的免疫算法、克隆选择算法、免疫学习算法等。近年来，基于免疫系统原理开发的各种模型和算法广泛地应用在科学研究和工程实践中，包括：信息安全、模式识别、数据挖掘和机器人学等方面。

参 考 文 献

[1] 肖人彬，王磊．人工免疫系统：原理、模型、分析及展望．计算机学报，2002,25(12)：1282-1293.

[2] 林学颜，张玲．现代细胞与分子免疫学．北京：科学出版社，1999.

[3] De Castro L N, Von Zuben F J. Artificial immune system:Part Ⅰ:basic theory and application. School of Electrical and Computer Engineering, State University of Campinas, Campinas-SR, Brazil:Technical Report RT-DCA 01,1999.

[4] 焦李成，杜海峰．人工免疫系统进展与展望．电子学报，2003,31(10)：1540-1548.

[5] Farmer J D, Packard N H, Perelson A S. The immune system, asaptation, and machine learning. Physica D, 1986:187-204.

[6] Smith D J, Forrest S, Perelson A S. Immunological memory is associative. In:Dasgupta ed. Artificial Immune Systems and Their Applications. Berlin:Springer,1998:105-112.

[7] Jerne N K. The immune system . Scientific American,1973,229(1):51-60.

[8] Burnet F M. Colnal selection and after . In: Bell G I, Perelson A S, Pimbley G H eds. Theoretical Immunology, New York: Marcle Dekker Inc.1978:63-65.

[9] De Castro L N, Von Zuben F J. Clonal selection algorithm with engineering applications. In:Proc GECCO'00, Las Vegas, Nevada, USA, 2000:36-37.

[10] Kim J, Bentley P. The artificial immune model for network intrusion detection . In: Proc 7th European Congress on Intelligent Techniques and Soft Computing, Aachen, Germany, 1999:13-19.

[11] Kim J, Bentley P. Towards an artificial immune system for network intrusion detection: An investigation of clonal selection with a negative selection operator. In:Proc Congress on Evolutionary Computation, Seoul,Korea,2001:27-30.

[12] 周志华，陈世福．神经网络集成．计算机学报，2002,25(1)：1-8.

[13] Jerne N K. Towards a network theory of the immune system. Annual Immunology, 1974,125C:373-389.

[14] Ishiguro A, Shirai Y, Kondo T et al.Immunoid: An architecture for behavior arbitration

based on the immune networks. In Proc IEEE/RSJ International Conference on Intelligent Robots and Systems, Osaka, Japan, 1996:1730-1738.

[15] Tang Z, Yamaguchi T, Tashima K et al.Multiple-valued immune network model and its simulations. In:Proc 27th Internation Symposium on Multiple-Valued Logic, Antigonish, Nova Scotia, Canada, 1997:519-524.

[16] Forrest S, Hofmeyr S A. Immunology as information processing. In:Segel and Cohen eds. Design Principles for the Immune System and Other Distributed Autonomous Systems. USA:Oxford University Press,2000.

[17] 蔡自兴，龚涛．免疫算法研究的进展．控制与决策．2004,19(8)：841-846.

[18] Forrest S, Perelson A S, Aleen L, Cherukuri R. Self-nonself discrimination in a computer. Proceedings of IEEE symposium on research in security and privacy.1994:202-212.

[19] 张剑，谢学科，何华灿，赵敏. 免疫计算的主要模型. 微电子学与计算机，2004,21(10)：93-96.

[20] De Castro, L N & Von Zuben, F J. An Evolutionary Immune Network for Data Clustering. In Proceedings of the IEEE SBRN'00,84-89.

[21] Timmis J, Mark Neal. A resource limited artificial immune system for data analysis. Knowledge Based Systems,June 2001,14(3-4):121-130.

[22] Hunt J E, Cooke D E. Learning using an artificial immune system. Journal of Network and Computer Applications,1996,19(2):189-212.

[23] Ishida Y. Fully Distributed Diagnosis by PDP learning algorithm towards immune network PDP model. In: Proc International Joint Conference on Neural Networks, San Diego, CA, USA, 1990:777-782.

[24] Forrest S,Hofmeyr S A, Somayaji A. Computer immunology. Communications of the ACM,1997,40(10):88-96.

[25] Dasgupta D, Cao Y, Yang C. Immunogenetic approach to spectra recognition. In:Proc GECCO'99, San Francisco,CA,USA,1999:149-155.

[26] Timmis J, Knight T. Artificial immunes system: Using the immune system as inspiration for data mining. In:Abbass H A, Sarker R A, Newton C S eds. Data Mining: A Heuristic Approach. Hershey:Idea Publishing Group,2001:209-230.

[27] Endoh S, Toma N, Yamada K. Immune algorithm for n-TSP. In:Proc IEEE International Conference on Systems, Man,and Cybernetics, San Diego, CA,USA,1998:3844-3849.

[28] 曹先彬，郑振，刘克胜等．免疫进化策略及其在二次布局求解中的应用．计算机工程，2000,26(3)：1-10.

[29] 曹先彬，刘克胜，王煦法．基于免疫遗传算法的装箱问题．小型微型计算机系统，2000,21(4)：361-363.

[30] Mori K, Tsukiyama M, Fukuda T. Adaptive scheduling system inspired by immune system. In Proc 1998 IEEE International Conference on Systems, Man, and Cybernetics, San Diego, 1998:3833-3837.

[31] Mitsumoto N, Hattori T, Idogaki T et al. Self-organizing micro robotic system. In: Proc 6th International Symposium on Micro Machine and Human Science, Nagoya,Japan, 1995:261-270.

Chapter 8

第8章 量子算法

从普朗克提出量子的概念至今，量子力学已经走过了整整一百年的历程。在这一百年中，量子力学给人类的生活带来了翻天覆地的变化[1]。

量子计算是应用量子力学原理来进行有效计算的新颖计算模式，它利用量子叠加性、纠缠性和量子的相干性实现量子的并行计算。量子计算从本质上改变了传统的计算理念[2]。

将量子计算内在的特性与传统的智能计算相结合，具有很好的发展潜力。量子计算理论应用于智能计算最早开始于专家系统，现在已应用到更多的智能计算中，如进化计算。

8.1 量子及基本特性

Feynman 认为，量子是一种既不具有经典粒子性，也不具有经典波动性的物理客体（如光子）。也有人将量子解释为一种量，它反映了一些物理量取值的离散性，其离散值之间的差值（未必为定值）定义为量子。按照量子力学原理，某些粒子存在若干离散的能量分布，称为能级。而某个物理客体（如电子）在另一个客体（如原子核）的离散能级之间跃迁（粒子在不同能量级分布中的能级转移过程）时将会吸引或发出另一种物理客体（如光子），该物理客体所携带的能量的值恰好是发生跃迁的两个能级的差值，这使得物理“客体”和物理“量”之间产生了一个相互沟通和转化的桥梁。爱因斯坦的质能转换关系也提示了物质和能量在一定条件下是可以相互转化的。因此，量子的这两种定义方式是对立统一并可以相互转化的。

量子的某些独特的性质为量子计算的优越性提供了基础[3]。

8.1.1 量子位[3,4]

在经典计算机中，信息单元用 1 个二进制位（bit）表示，它处于“0”态或“1”态。而在二进制量子机中，信息单元称为“量子位”，它除了可以是处于“0”态或“1”态外，还可以处于一种叠加态（State of Superposition）。叠加态是“0”态和“1”态的任意线性叠加，它以一定的概率同时存在于“0”态和“1”态之间。量子叠加态通过测量或与其他物体发生相互作用而呈现出“0”态或“1”态。任何具有两态的量子系统都可用来实现量子位。

一个量子系统包含若干粒子，这些粒子按照量子力学的规律运动，称此系统处于态空间的某种量子态。态空间由多个本征态（Eigenstate）（即基本的量子态）构成，基本量子态简称基本态（Basic State）或基矢（Basic Vector）。态空间可用 Hilbert 空间（线性复向量空间）来表述，即 Hilbert 空间可以表述量子系统的各种可能的量子态。

为了便于表示和运算，Dirac 提出用符号$|x\rangle$来表示量子态，$|x\rangle$是一个列向量，称为右矢（ket）；它的共轭转置用$\langle x|$表示，$\langle x|$是一个行向量，称为左矢（bra）。一个量子位的叠加态可用二维 Hilbert 空间（即二维复向量空间）的单位向量$|\psi\rangle$来描述。在这个空间里，$|\psi\rangle$可写成：$|\psi\rangle = a|\uparrow\rangle + b|\rightarrow\rangle$，式中$|\uparrow\rangle$和$|\rightarrow\rangle$是量子位的基本态，它们正交；$a$和$b$为概率振幅（Probability Amplitude），它们是复数；$|a|^2$和$|b|^2$分别表示$|\psi\rangle$为$|\uparrow\rangle$态和$|\rightarrow\rangle$态的概率，且$|a|^2+|b|^2=1$，这表明$|\psi\rangle$是单位向量，也称$|\psi\rangle$是归一化的（Nomalized）。在常规计算机中，一个数位的态是确定性的（Deterministic），而在量子计算机中，量子位的叠加态不是确定性的，而是概率性的（Probabilistic）。

当$|\psi\rangle$对$|\uparrow\rangle$投影时，$|\psi\rangle$变成$|\psi\rangle_{\uparrow}$，$|\psi\rangle_{\uparrow} = a|\uparrow\rangle$，这相当于在$|\uparrow\rangle$方向对$|\psi\rangle$进行测量。同样，当$|\psi\rangle$对$|\rightarrow\rangle$投影时，$|\psi\rangle$变成$|\psi\rangle_{\rightarrow}$，$|\psi\rangle_{\rightarrow} = b|\rightarrow\rangle$，这相当于在$|\rightarrow\rangle$方向对$|\psi\rangle$进行测量。所以，当对处于叠加态的量子位进行观察或测量时，叠加态将受到干扰，并发生变化，这种变化称为坍缩。对于上述测量，叠加态坍缩为基本态。

在二维 Hilbert 空间，对于$x, y \in \{0,1\}$，$\langle x|y\rangle = (\langle x|, |y\rangle)$称为内积，它是一个标量；而$|x\rangle\langle y|$称为外积，它是一个算符。

在量子计算中，关于矩阵之间的操作，引入了张量积（Tensor Product），这是由于一个复合量子计算系统与几个独立的量子计算子系统之间的关系可以方便地用张量积进行描述，且张量积还将有利于几个叠加态的合并。令H_1和H_2是以B_1和B_2为基的两个 Hilbert 空间，则其上的张量积运算可定义为：

$$H = H_1 \otimes H_2 = \{\sum_{|i\rangle \in B_1} \sum_{|j\rangle \in B_2} c_{ij} |i, j\rangle \mid c_{ij} \in C\} \tag{8.1}$$

其中，H 是以 $B_1 \times B_2$ 为基的 Hilbert 空间。

8.1.2　量子纠缠

量子纠缠是存在于多子系统的量子系统中的一种奇妙现象，即对一个子系统的测量结果无法独立于对其他子系统的测量参数[5]。若一个量子计算系统中若干量子位的态不能表示成子状态的张量积的形式，则称这些量子位处于纠缠态。纠缠态首先在 1935 年由 Einstein[6]等人提出，量子纠缠的物理原理目前尚不清楚，一般认为量子纠缠是一种介于经典关联和量子相干关联之间的一种强关联状态。例如，Bell 态 $\frac{1}{\sqrt{2}}|0,0\rangle+\frac{1}{\sqrt{2}}|1,1\rangle$ 就是一个典型的纠缠态。其中的两个量子位无法写成张量积形式；而 $\frac{1}{\sqrt{2}}|0,0\rangle+\frac{1}{\sqrt{2}}|0,1\rangle$ 就不是纠缠态，因为它可以用张量积表示为 $|0\rangle\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$。当多个量子位处于纠缠态时，对部分量子位的态的测量将影响其他量子位的态，即便这些量子位分别处于不同的空间位置。量子纠缠是一种有用的信息资源，在量子隐态传输、量子超密编码、量子密钥分配，以及在量子计算的加速、量子纠错、防错等方面都起着重要作用。

量子纠缠态使量子计算机具有更大的优越性，相隔很远的两个纠缠的量子态具有瞬时相关性，改变其中的一个状态另一个状态则立即随之变化，这种关系跨越了空间和时间，理论上通过两个纠缠态量子单元之间的通信速度可以超越光速[3]。

8.1.3　量子克隆[5]

量子态不可克隆是量子力学的固有特性，它设置了一个不可逾越的界限。量子不可克隆定理是量子信息科学的重要理论基础之一。量子信息是以量子态为信息载体（信息单元）的。量子态不可精确复制是量子密码术的重要前提，它确保了量子密码的安全性，使得窃听者不可能采取克隆技术来获得合法用户的信息。鉴于这个定理的重要性，近年来人们对它做了进一步的研究，揭示出更丰富的物理内涵。量子不可克隆定理断言，非正交态不可克隆，但它并没有排除非精确克隆即复制量子态的可能性。目前主要有两种克隆机：普适量子克隆机和概率量子克隆机。

普适量子克隆机（Buzek-Hillery 克隆机）中常用的态是保真度。普适量子克隆机对于任意的量子态都适用。其性能与输入态无关，且两个输出态完全相同，但不等于输入态，这表明输入态在复制过程中不可避免地遭到破坏。选择一组最佳参数可使得这种破坏降到最小程

度，已经证明，输入、输出态之间的保真度最高可以达到 5/6。

概率量子克隆机适用于线性无关的态集。它把幺正演化和测量过程相结合，以确定的大于零的概率产生输出，而且输出态一定是输入态的精确复制态。为构造概率量子克隆机，测量和合适的幺正演化都是不可缺的。如果只有幺正演化，显然非正交态不可以精确克隆；另一方面，如果只有测量，当输入态为非正交态时，机器不可能对其中任意一个输入态都以大于零的概率产生输出，且输出态还是输入态的精确复制态。因此构造概率量子克隆机的关键是要设计出合适的幺正演化并要联系测量过程。概率量子克隆机成功产生输出的概率，定义为克隆效率，它决定了该机器的性能。显然，对于确定的输入态集合，希望设计一种机器，使得它具有最大效率，且该效率不依赖于具体的输入态，此时，该机器称为最佳概率量子克隆机。已经证明，只有对于正交输入态，才可以使得效率达到 1。

8.2 量子智能算法

量子算法的核心就是利用量子的各种特性来加速求解速度，达到经典计算机不可比拟的运算速度和信息处理能力。目前有三类优于已知传统算法的量子算法：①基于 Fourier 变换的量子算法，包括 Deutsch-Jozsa（DJ）算法和 Shor 的因子分解算法及离散对数算法；②Grover 的量子搜索算法；③量子仿真算法，用量子计算机模拟量子系统。

而量子智能计算是近几年来引起极大兴趣的研究方向。它有效地利用了量子理论原理并结合了传统智能计算的优势。目前的研究领域包括量子神经网络、量子遗传计算、量子退火计算、量子克隆计算、量子免疫计算、量子聚类计算及量子小波计算等[2]。

8.2.1 量子神经网络[7~10]

神经计算是通过对人脑工作原理的简单模仿，建立在简化的神经元模型和学习规则基础之上的一种计算范式。它特殊的拓扑结构和学习方式产生了许多计算上的优势，主要体现在并行计算、分布式信息处理，以及从输入到输出的非线性映射等方面，这些特点已拥有许多非常成功的应用。但是，随着信息处理量和复杂度的增加，神经计算的局限与不足也逐渐凸显出来，主要表现在：①当在信息量大的情况下学习时处理速度过慢，不符合人脑实时反应、大容量作业的特征；②人工神经网络的记忆容量有限；③人工神经网络需要反复训练，而人脑却具有一次学习的能力；④人工神经网络在接受新的信息时会发生灾变性失忆现象等。这些本质上的缺陷使得人们对于传统神经计算理论的进一步发展提出了强烈的要求，于是便出现了神经计算与其他理论相结合的实践，这其中与量子计算的结合具有非常好的前景，是当

前人工神经网络理论发展的一个前沿课题，由此而产生的量子神经计算新范式有着很高的理论价值和应用潜力。

量子神经计算的概念是由美国 Louisiana 州立大学的 Kak 教授在 1995 年提出的，开创了该领域的先河。神经计算与量子理论的结合可以有多种形式，由此而产生的计算模型也各有特点。

虽然目前国际上量子神经计算及其模型（量子神经网络）的研究还处于萌芽阶段，但也有少数先行者提出了诸如量子联想、并行学习、经验分析等新概念，开创了量子神经网络新的交叉学科。就量子理论与神经网络技术结合的形式而言，大致有两种：一种是在神经网络的结构或训练过程中引入量子理论，从而提高神经网络的学习和推广能力；另一种则是直接借用量子理论中的某些原理或概念，来指导设计神经网络拓扑结构或训练算法。

1．量子神经元模型

在经典人工神经网络模型中最简单的是感知机，它以 n 个二进制数集 $\{i_j\}$ 作为输入值，还定义了连接权矢量 $\boldsymbol{W}=[\omega_1,\omega_2,\cdots,\omega_n]^{\mathrm{T}}$，阈值 θ 和激活函数 f：

$$f=\begin{cases}1 & \text{若}\sum_{j=1}^{n}\omega_j i_j>\theta\\ -1 & \text{其他}\end{cases} \tag{8.2}$$

该模型无法解决线性不可分问题，但其形式和性质简单，因此能够研究它的量子对照物，即量子神经元模型。在量子神经元模型中，同样取 $\{i_j\}$ 作为输入，单个连接权矢量被一个波函数 $\psi(w,t)$ 所取代，其余部分皆与经典模型类似。这里的波函数处于 Hilbert 空间，其基态为经典模型的权矢量，$\psi(w,t)$ 代表了权矢空间中所有可能权矢的概率幅度（广义上为复数），在任意时刻 t 满足归一化条件，即 $\int_{-\infty}^{\infty}|\psi|^2\mathrm{d}\omega=1$。

于是，感知机的权矢就被许多权矢的量子叠加所代替，不过，一旦当它与环境发生作用时将立即坍缩到其中之一的经典权矢之上，且概率为 $|\psi|^2$。

2．量子衍生神经网络

在神经网络设计、开发和实现过程中这种方法使用了量子理论的“多宇宙”观点。在训练一个传统的神经网络时需要反复学习模式集，直到网络对每个模式达到合适的输出为止，不过这种模式的重复出现（有时是成百上千次的）并无人类学习的生物基础。由量子“多宇宙”概念衍生出的神经网络方法则认为，训练集中的模式犹如一个粒子，在不同的宇宙中被大量分离的神经网络（可能是同种类型也可能不是）所处理，类似于一个光子同时穿过许多

窄缝，而训练集中的每个模式仅在自身宇宙中被处理。这样，实际上就需要许多神经网络同时进行训练，网络个数应等于训练模式数。每个网络与其相关的训练模式存在于一个分离的宇宙，一旦每个网络在其宇宙中训练成功，就计算这些网络的量子叠加态，由此推导出一个量子衍生神经网络（QuINN），把它推广到所有输入模式中，而结果的叠加权矢量称为量子衍生函数（QuIWF），它坍缩到实际输入模式，具体坍缩依赖于输入模式和坍缩模式。

对于网络的量子叠加方法有不同的观点。Fermion 的观点认为单个粒子的波函数相互之间不发生重叠，当坍缩发生时某个存在的宇宙（即训练过的网络）就是结果；而 Boson 观点则认为波函数可以相互交叠，相应的宇宙相互融合，并且可以坍缩到一个在训练过程中并不独立存在的网络之中。实验结果表明，利用“多宇宙”观点来设计和训练神经网络，在某些场合会提供更快的训练速度，同时又无泛化能力的损失。此外，量子衍生神经网络具有消除灾变性失忆的潜力，这是因为一个网络训练一个模式，因此在训练过程中模式之间不发生相互干扰。与此同时，QuINN 还为线性不可分问题提供了一个单层网络的解决方案。

3．量子并行 SOM 模型

量子并行 SOM 模型是针对并行计算环境，通过对传统的 Kohonen-SOM 模型进行改进后得到的，此模型用来模拟人脑的一次学习和记忆功能。在训练过程中，输入、输出层神经元之间的每个连接分别作为一个独立的处理器（共有 $M \times P$ 个， M 为输入信号所有元素数， P 为数据可能的分类数），这样每个矩阵的所有元素便可以同时进行计算，极大地提高了权值更新的能力。

与传统 SOM 算法比较，该模型主要有以下改进：①输入和输出层中神经元及它们之间的连接数目等于输入信号所有元素数与数据可能的分类数的乘积；②在一对输入和输出神经元之间只有一个连接，每个连接可看做一个独立工作的处理器；③权值更新被视为一定次序的矩阵相乘，它适合于并行处理。

8.2.2 量子进化算法

量子进化算法（QEA）是量子计算与进化计算相结合的产物，它建立在量子态矢量表达的基础上，将量子比特的概率幅表示方式应用于染色体的编码，使得一个染色体可以表达多个模态的叠加，从而比传统的进化计算更具并行性。同时，QEA 利用当前最优个体的信息来更新量子旋转门，以加速算法收敛，若进一步引入量子交叉、变异和灾变等操作，则可以克服早熟收敛现象。

量子进化算法的基本特征主要体现在以下几个方面：①由特殊的量子位表示形式带来的种群多样性；②从量子位表示形式到二进制编码的转换机制；③通过量子旋转门的驱动向最

优解的进化过程；④以量子位个体概率幅的分散性为目标的个体移民策略；⑤以算法收敛到最优解的概率为依据的终止准则。也就是说，在量子进化算法中，染色体不是用确定性的值表示的，譬如二进制串、浮点数、实数等，而是采用量子位（Q-bit）或概率幅的方式表示的。

量子进化算法具有如下优点：①算法通用，不依赖问题信息；②算法原理简单，容易实现；③种群分散性好，小种群染色体可以对应多个搜索状态；④种群搜索，具有极强的全局搜索能力；⑤算法利用当前最优个体的信息驱动进一步的搜索，即协同搜索；⑥收敛速度快，能够很快地发现最优解[11]。

类似于进化计算，可以将量子进化计算分为量子遗传算法、量子进化规划和量子进化策略。

1．量子遗传算法[12]

1）量子比特编码

在量子计算机中，充当信息存储单元的物理介质是一个双态量子系统，称为量子位（Q-bit）。通常，一个量子位可表示如下：

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \tag{8.3}$$

其中，α 和 β 为复数，分别表示状态 $|0\rangle$ 和 $|1\rangle$ 的概率幅。从而 $|\alpha|^2$ 和 $|\beta|^2$ 表示了该量子位处于状态 0 和状态 1 的概率大小。显然，必须满足归一化条件 $|\alpha|^2+|\beta|^2=1$。因此，一个长度 m 维的量子染色体可表示为：

$$\begin{pmatrix}\alpha_1 & \alpha_2 & \cdots & \alpha_m\\ \beta_1 & \beta_2 & \cdots & \beta_m\end{pmatrix} \tag{8.4}$$

其中，$|\alpha_i|^2+|\beta_i|^2=1$，$i=1,2,\cdots,m$。

考虑如下长度为 3 的量子染色体：

$$\begin{pmatrix}1/\sqrt{2} & 1/\sqrt{2} & 1/\sqrt{2}\\ 1/\sqrt{2} & -1/\sqrt{2} & \sqrt{3}/2\end{pmatrix}$$

其表示的量子位状态为：

$$\frac{1}{4}|000\rangle+\frac{\sqrt{3}}{4}|001\rangle-\frac{1}{4}|010\rangle-\frac{\sqrt{3}}{4}|011\rangle+\frac{1}{4}|100\rangle+\frac{\sqrt{3}}{4}|101\rangle-\frac{1}{4}|110\rangle-\frac{\sqrt{3}}{4}|111\rangle$$

这意味着量子位状态取 $|000\rangle$，$|001\rangle$，$|010\rangle$，$|011\rangle$，$|100\rangle$，$|101\rangle$，$|110\rangle$ 和 $|111\rangle$ 的概率分别为 1/16，3/16，1/16，3/16，1/16，3/16，1/16，3/16。因此，长度为 3 的量子染色体个体

同时包含了 8 个量子位状态的信息。正是这种表示形式，使得单个染色体可表达多个状态的线性叠加，从而使采用量子位表示的进化算法有着优越的种群多样性特征。

2）量子遗传算法流程

（1）令 $t=0$，随机产生 N 个初始个体，以构成种群 $P(t)=\{p_1^t,\cdots,p_N^t\}$，其中，$p_j^t$ 为第 t 代种群中的第 j 个个体，即

$$p_j^t=\begin{pmatrix}\alpha_1^t & \alpha_2^t & \cdots & \alpha_m^t\\ \beta_1^t & \beta_2^t & \cdots & \beta_m^t\end{pmatrix} \tag{8.5}$$

m 为量子位数目，即量子染色体的长度。

（2）根据 p_j^t 中概率幅的取值情况构造长度为 m 的二进制串 r_j^t。首先产生 0～1 之间的一个随机数 s，若 $|\alpha_i^t|^2>s$，则对应位置取值为 1；否则取 0。由此，得到二进制串构成的种群 $R(t)$。

（3）进行个体交叉、变异操作，生成新的 $R(t)$。

（4）评价 $R(t)$ 中的各个体，并保留最优个体 b。若满足终止条件，则终止算法；否则，继续以下步骤。

（5）更新 $P(t)$。

（6）令 $t=t+1$，并返回（2）。

3）量子变异

和普通编码方式不同，QGA 中的染色体是一种概率表示，因此对概率的交叉是没有物理意义的，所以变异是作用于量子染色体的唯一遗传算子，下面给出两种量子变异。

（1）量子变异 1。

GA 中通常的变异操作是一种随机变动，个体的进化带有随机扰动因素，而没有利用进化历史中的有利信息。简单的变异量子染色体的方法，可有效利用当代的信息，由当前最优解中反推出一个量子染色体的概率分布，类似于一种概率遗传算法，但是操作过程却简单得多。算法可简单地这样描述：根据当前最优个体推出一个指导量子染色体后，在它的周围随机散布量子染色体作为下一代的量子种群。用公式表示为：

$$Q_g(t)=a\times p_c(t)+(1-a)\times(1-p_c(t)) \tag{8.6}$$

$$\theta(t+1)=Q_g(t)+b\times\text{normrnd}(0,1) \tag{8.7}$$

其中，$p_c(t)$ 为到第 t 代为止的最优个体；Q_g 为指导量子染色体；a 为 $p_c(t)$ 的影响因子；b 为量子种群随机散布的方差。采用上述的观察方式，要以概率 1 得到染色体 $p=(1\ 1\ 0\ 0\ 1)$，只需令量子染色体 $Q=(0\ 0\ 1\ 1\ 0)$，即 $Q=\overline{p}$。如果 p 是搜索空间中的最优解，则种群中的量子染色体越接近 Q，得到最优解的概率越大。a 的值越小，量子种群受 Q_g 的影响越大，但

a=0 时，$Q_g=\overline{p}$，观察 Q_g 后将以概率 1 得到 p。一般取 $a\in[0.1,0.5]$，$b\in[0.05,0.15]$。

（2）量子变异 2。

在量子理论中，状态间的转移是通过量子门变换矩阵来实现的。量子门的构造是设计算法的关键，直接影响着算法的性能。量子门的设计有多种形式，如非门、受控非门、Hadamard 门等。最常用的量子门为：

$$\begin{pmatrix}\alpha_i'\\ \beta_i'\end{pmatrix}=U(\theta_i)\begin{pmatrix}\alpha_i\\ \beta_i\end{pmatrix}=\begin{pmatrix}\cos\theta_i & -\sin\theta_i\\ \sin\theta_i & \cos\theta_i\end{pmatrix}\begin{pmatrix}\alpha_i\\ \beta_i\end{pmatrix} \tag{8.8}$$

$U(\theta_i)$ 表示量子旋转门，旋转角度 θ_i 可由表 8.1 得到。

表 8.1　旋转角度 θ_i

x_i	b_i	$f(x)\geqslant f(b)$	$\Delta\theta_i$	$s(\alpha_i\beta_i)$			
				$\alpha_i\beta_i>0$	$\alpha_i\beta_i<0$	$\alpha_i=0$	$\beta_i=0$
0	0	假	0	0	0	0	0
0	0	真	0	0	0	0	0
0	1	假	0	0	0	0	0
0	1	真	0.01π	−1	+1	±1	0
1	0	假	0.01 π	−1	+1	±1	0
1	0	真	0.01 π	+1	−1	0	±1
1	1	假	0.01 π	+1	−1	0	±1
1	1	真	0.01 π	+1	−1	0	±1

其中，x_i 和 b_i 为当前染色体和当前最优染色体的第 i 位；$f(x)$ 为适应度函数，$\Delta\theta_i$ 为旋转角度，控制算法收敛速度；$s(\alpha_i\beta_i)$ 为旋转角度的方向。举例说明量子旋转门的构造。例如，当 x_i=0，b_i=1，$f(x)\geqslant f(b)$时，为使当前解收敛到一个具有更高适应度的染色体，应增大当前取 0 的概率，即要使$|\alpha_i|^2$ 变大。若 (α_i,β_i) 在第 1，3 象限，则 θ_i 应向顺时针方向旋转；若 (α_i,β_i) 在第 2，4 象限，则 θ_i 应向逆时针方向旋转。

由于量子位的特殊表示形式，一个量子个体可以表示若干个量子位状态的叠加，从而一个小种群的量子个体可对应于传统表示方法下很大数量的个体。同时，量子门操作的存在，使得量子遗传算法有着极强的全局搜索能力。另外，随着 QGA 的收敛，各个量子位上取 1 或取 0 的概率幅将趋于 1，由量子旋转门驱动的搜索过程将自动地由全局搜索变为局部搜索，这使得算法取得了粗搜索（Exploration）与细搜索（Exploitation）能力的均衡。这些特征正是由量子算法内在的概率机制所决定的。

2．量子进化规划[13]

进化规划对生物进化过程的模拟是着眼于物种的进化过程，不使用个体重组算子，所以变异是进化规划的唯一搜索最优个体的方法，最常用的是高斯变异算子。可以证明，若采用高斯变异算子产生后代，进化规划可以渐进收敛到问题的全局最优解。它的缺点是进化求优的时间一般很长。而量子进化规划采用表 8.2 所示的量子变异。

表 8.2 量子变异

$x_i > \text{best}_i$	$x_i = \text{best}_i$	$x_i < \text{best}_i$	$f(x) > f(\text{best})$	$\Delta\theta_i$
0	0	1	0	-0.01π
0	0	1	1	-0.001π
0	1	0	1	$\pm 0.01\pi$
1	0	0	0	0.01π
1	0	0	1	0.001π

其中，x_i 和 best_i 分别为当前染色体和当前最优染色体；$f(x)$ 为适应度函数；$\Delta\theta_i$ 为旋转角。量子进化规划可以如下描述：

（1）根据求解的精度确定搜索空间的维数，假设搜索空间 Ω 是一个 n 维空间，与此相对应，搜索点就是一个 n 维向量，然后随机生成初始种群 $Q(t)$。

（2）由 $Q(t)$ 生成 $P(t)$。

（3）对当前的父代群体进行变异操作得到 $Q'(t)$，由 $Q'(t)$ 生成新个体 $P'(t)$。

（4）计算当前第 t 代父本种群的适应度，采用联赛方法选择。

（5）判断停机条件，$Q(t) = Q'(t)$，$t = t + 1$，转至（2）。

3．量子进化策略[14]

20 世纪 60 年代，柏林理工大学的 Rechenberg 和 Schwefel 等人在对生物进化的研究成果进行分析与理解的基础上，借鉴其相关内容和知识，特别是遗传进化方面的理论与概念，针对处理流体力学中弯管形态的优化问题，提出并发展了一种新的优化算法——量子进化策略。量子进化策略就是把量子进化算子引入到进化策略中。其算法过程与量子进化规划大致相同。

4．量子进化算法的改进[11]

目前，量子进化算法的改进研究工作主要可归纳为如下几个方面。

1）改进基本算子

基本 QGA 通过量子门实现进化操作，因此改进往往从量子门的旋转操作着手。Han 等人对原有量子旋转门在概率幅趋近于 1 或 0 的情况进行了修正，提出一种基于 Hε 门的旋转门操作，使得算法可有效避免陷入局部极小。量子旋转门操作需要多次比较和计算才可以确定旋转角，因此算法的计算量和复杂性较大。Chen 等人提出了一种混沌更新旋转门，用以替代原有的量子旋转门操作。实际上，量子概率幅本身具有混沌特性，而量子旋转门操作则是为了完成进化操作，并使量子概率幅随着算法的收敛由混沌向确定转化。因此，采用预先生成的混沌序列来更新量子门可大幅度减少计算量。进而提高算法在实时环境下的使用能力。另外，Chen 等人在 Jordan 构造的理论框架下，证明了基于其混沌旋转门的 QGA 的完全收敛性。此外，Yang 等人提出了一种算术形式的量子旋转门操作，采用当前最好个体作为量子旋转的指导，并将该个体所带有的信息在下一代种群中进行分享。

2）引入新算子

基本 QGA 步骤中没有传统的遗传操作，因此可通过引入交叉、变异、灾变等遗传算子来改善算法的性能。Li 等人对 QGA 进行了改进，提出了基于量子概率表达的一种遗传算法，其核心是利用量子概率编码个体的独立搜索能力，通过多个个体同时搜索来增强算法的搜索性能，并设计了一种新的交叉算子和一个单量子比特变异算子。Yang 等人引入量子非门作为变异操作，依一定的概率从种群中选择一个或多个个体，然后随机选择一个或多个位置实施变异。Li 等人在基本 QGA 中引入了量子交叉和变异，用以克服早熟收敛的问题，增强算法搜索能力。Yang 等人借鉴量子相干特性，提出了一种全干扰交叉算子，同时引入多个个体进行交叉操作，将多个个体的染色体拆开，依照预先拟定的准则重组，以构造新的个体，即使在多个交叉个体完全相同的极端情况下，该交叉操作也可以产生新个体。

基本 QGA 利用量子旋转门进行种群的进化，同时通过观察量子染色体的状态来生成所需要的二进制解。Li 等人认为这一概率操作过程具有很大的随机性和盲目性，个体在进化的同时存在着退化的可能。同时，每个实际问题都会有一定的特征信息或先验知识，但基本 QGA 却忽视了这些信息对求解问题的帮助作用。为此他们引入了免疫算子，并应用于待评价的种群中。另外，Wang 等人除了在 QGA 中引入遗传操作外，还引入了灾变操作，从而增强了算法避免陷入局部极小的能力。

3）改变种群规模

传统遗传算法中染色体与解之间是一对一关系，而 QGA 则可采用一个染色体表示多解。因此，算法可以用较小的种群规模表示问题的多个解。Talbi 等人将“小生境”概念引入基本量子遗传算法，并应用于旅行商问题。该算法中，初始种群仅包含 4 个路径生成矩阵，且每个矩阵的每个元素均用量子位表示。算法运行过程中，由量子位表示的矩阵生成若干个可行路径矩阵，然后通过交叉、变异、矩阵内各行随机移动等操作来生成新的个体。对于种群的

更新，算法选取 3 个最优个体，并随机选择 1 个来保持种群的多样性。该算法充分利用了量子位表示方式可表示多个解的特性，保持解种群的分散特性。

4）扩展为并行算法

QGA 的表示形式决定了种群中的每个个体可以同时表示多个状态。但是，在基本 QGA 中种群的每个个体仅由其本身概率幅和当前最好解个体决定，个体与个体之间的联系不紧密。因此，将整个种群划分为若干个子种群，每个子种群独立进行进化操作，并在一定的进化代数之后进行个体的交换，即采用所谓“移民”操作来传递信息，如此可实现并行算法。Han 等人在基本 QGA 的基础上，引入了两种“移民”策略，以加强种群个体之间信息的交互，其中包括“局部移民”操作和“全局移民”操作。前者用于将搜索得到的优秀解所包含的信息在种群个体间进行交互；后者用于将搜索得到的优秀解所包含的信息在种群个体与最优解个体间进行交互。另外，Han 等人分别设计了针对 4 个和 16 个处理单元信息的“星型”交互结构，采用粗粒度并行策略进行最优解个体的交互。Zhang 等人也提出了一种新型的粗粒度并行 QGA，采用一种“分等级环形模型”的交互式结构。Yang 等人提出了一种多宇宙并行 QGA，将所有个体按照一定的拓扑结构分成一个个独立的子群体。Li 等人基于粗粒度模型，提出了一种结合并行量子进化算法和局部搜索算法的混合算法。

5）构造新型算法框架

Han 等人研究发现，量子位的初始值对 QGA 的性能有着显著的影响，并由此提出了一种 2 阶段的复合 QGA 框架。在第 1 阶段中随机初始化量子位，经过若干次量子进化搜索后，将所得到的优良结果用于第 2 阶段 QGA 的初始化，进行进一步解空间的全局搜索。Wang 等人提出了混合 QGA 的框架，在该混合算法中，纵向为 QGA 基于量子门更新的搜索过程，横向则是传统遗传算法基于二进制、实数编码或组合空间的遗传搜索过程。基于不同的解表征空间上搜索的混合，以及基于不同的解表征方式的多种遗传操作的混合，有利于丰富搜索行为，增强搜索能力，进而避免早熟收敛。同时，算法还将纵向 QGA 得到的优良结果与横向传统遗传算法上代的搜索结果采用整体保优策略进行更新，从而可避免优良解的遗失，并加快种群的整体收敛过程。从某种意义上来说，这种算法框架融合了微观空间和宏观空间上的搜索，增强和均衡了全局与局部搜索能力，因而具有优良的性能。

8.3 小结

量子计算是应用量子力学原理来进行有效计算的新颖计算模式。将量子计算内在的特性与传统的智能计算相结合，具有很好的发展潜力。

量子具有量子位、量子纠缠、量子克隆等基本特征。量子算法就是利用量子的各种基本

特性来加速求解速度的算法。目前有三类优于已知传统算法的量子算法：①基于 Fourier 变换的量子算法，包括 Deutsch-Jozsa（DJ）算法和 Shor 的因子分解算法及离散对数算法；②Grover 的量子搜索算法；③量子仿真算法，用量子计算机模拟量子系统。

量子智能计算有效地利用了量子理论原理并结合了传统智能计算的优势。目前的研究领域包括量子神经网络、量子遗传计算、量子退火计算、量子克隆计算、量子免疫计算、量子聚类计算及量子小波计算等。

参 考 文 献

[1] 周正威，黄运锋，张永生，郭光灿．量子计算的研究进展．物理学进展，2005,25(4)：368-385.
[2] 郑建国，覃朝勇．量子计算进展与展望．计算机应用研究，2008,25(3)：641-645.
[3] 吴楠，宋方敏．量子计算与量子计算机．计算机科学与探索，2007,1(1)：1-16.
[4] 夏培肃．量子计算．计算机研究与发展，2001,38(10)：1153-1171.
[5] 郭光灿．量子信息引论．物理，2001,30(5)：286-293.
[6] Einstein A, Podolskey B, Rosen N. Can quantum-mechanical description of physical reality be considered complete? Physical Review,1935,47:777-780.
[7] 解光军．量子神经计算．合肥工业大学学报（自然科学版），2002,25(3)：354-359.
[8] 解光军，庄镇泉．量子神经网络．计算机科学，2001,28(7)：1-6.
[9] 解光军．量子神经计算技术．吉首大学学报（自然科学版），2005,26(1)：3-7.
[10] KAKS C. On Quantum Neural Computer. Information Sciences,1995,83:143-160.
[11] 王凌．量子进化算法研究进展．控制与决策，2008,23(12)：1321-1326.
[12] 杨俊安，庄镇泉．量子遗传算法研究现状．计算机科学，2003,30(11)：13-15.
[13] 杨淑媛，焦李成，刘芳．量子进化算法．工程数学学报，2006,23(2)：235-246.
[14] 杨淑媛，刘芳，焦李成．量子进化策略．电子学报，2001,29(12A)：1873-1877.

Chapter 9

第9章 信息融合技术

9.1 信息融合技术的形成与发展

9.1.1 信息融合的定义及其必要性

信息融合技术是研究如何加工、协同利用多源信息，并使不同形式的信息相互补充，以获得对同一事物或目标更客观、更本质认识的信息综合处理技术。多传感器系统能完善地、精确地反映检测对象特征，消除信息的不确定性，提高传感器的可靠性。经过融合的多传感器信息具有冗余性、互补性、实时性及低成本性的特点。

信息融合的概念很好理解，但是“融合”的精确含义在各个应用领域中可能相差甚远。目前，要给出信息融合的一个统一的、精确的定义是非常困难的，这种困难是由其所研究的内容的广泛性和多样性带来的。首先，信息融合包括很多领域，这么宽泛的领域使它的定义不能局限于特定的应用、特定的采集方法。其次，融合过程需要用到不同的数学工具，因而也不能从这些工具的角度对融合进行定义。

信息融合最早用于军事领域，美国军方成立的数据融合工作组联合指导实验室（Joint Director Laboratories，JDL）给出一个定义为：数据融合是一个处理探测、互联、相关、估计，以及组合多源信息和数据的多层次、多方面的过程，目的是获得准确的状态和身份估计，完整而及时的战场态势和威胁估计。这一定义强调了信息融合的三个核心方面[1]：

（1）信息融合是在几个层次上完成对多源信息处理的过程，其中每一个层次都具有不同级别的信息抽象。

（2）信息融合包括探测、互联、相关、估计及信息组合。

（3）信息融合的结果包括较低层次上的状态估计和身份估计，以及较高层次上的整个战术态势估计。

由欧洲遥感实验室协会（European Association of Remote Sensing Laboratories，EARSeL）及法国电气和电子协会（French Society for Electricity and Electronics，IEEE 的法国机构）建立的一个工作组提出的数据融合在遥感领域的定义为：数据融合是一个由方法和工具表示的框架，用于进行不同来源的数据的联合。融合的目的是获得更高质量的信息；“更高质量”的精确含义依赖于它的具体应用。这一定义把融合定义的重点放在框架上，并强调了遥感中的数据融合的基本原则，而没有像其他定义那样，把重点放在工具和方法本身上。而且，这一定义强调了在许多信息融合的文献中被忽视的“质量”问题。在这里，“质量”一词表示执行融合过程比没有经过融合所得到的结果会令“用户”（Customer）更加满意。例如，更好的质量可以是分类精度的提高，也可以是相关信息的更好的利用结果，或者是整个操作过程的鲁棒性的提高。更高的质量也可以是对感兴趣的范围的更适合的覆盖面、项目相关的人力或物力资源的更合理的运用。在这一定义中，同一传感器的不同光谱信道，以及不同时刻采集的图像都可以是不同的信源。因此，对同一传感器得到的图像的处理也可以看做属于数据融合领域，如多光谱图像的分类，就是利用同一传感器的其他波段对光学波段进行大气层的修正的。另外，对同一传感器或不同传感器的时序数据的处理也可以看做是一个融合过程。

综合考虑以上几个定义，“融合”都是将来自多传感器或多源的信息和数据进行综合处理，从而得出更为准确可信的结论。这一综合过程有各种名称，如相关（Correlation）、合成（Integration）、混合（Commixture）、合并（Merging）、协同（Synergy），当然也包括融合，目前已统称为信息融合或数据融合。“融合”是一种非数学的术语，意指“组合或综合成一个整体”的过程，使用“融合”一词就避免了“相关”或“合成”这样的术语。相关和合成只是融合过程中执行的不同数学运算。另外，根据数据和信息的含义，由于信息融合更具概括性，用信息融合比较合适。由于习惯上的原因，很多文献仍沿用数据融合。当然，这里的“数据”已被扩展了，在有些情况下，如在智能融合时，它可以表示信息，甚至表示知识。本书将统一使用“信息融合”这一术语。

由于多源信息是关于同一对象的不同（或相同）侧面的有关信息，所以这些信息的相关是必然的，也是必要的。当一组多源信息的每个源以不同的可信度采集对象的同一个特征时，这组多源信息提供了冗余信息。由于每个源的噪声并不是完全相同的，因此将这组冗余信息进行融合，能降低总的不确定性，提高精度。并且由于冗余信息的存在，当一个甚至几个信息源出现故障时，系统仍可以利用其他信息源获取对象的信息，以维持系统的正常运转，使

系统具有容错性能；当各个信息源所提供的信息是被感知特征空间中的各个相互独立的子空间时，这些信息就是互补信息。互补信息能够提供完整描述对象的能力，互补信息描述了对象中的多个不同特征，因而能减少对对象模型理解的歧义，提高系统正确决策的能力，并且这种互补性经过适当处理后可以补偿单一信息源的不准确性和测量范围的局限性，提高信息获取的速度。在同等数量的信息源下，多源信息融合处理与各个信息源分别单独处理相比，由于多源信息融合可以使用并行结构，采用分布式系统并行算法，因此可显著提高信息处理的速度，降低信息获取的成本。信息融合提高了信息的利用效率，可以用多个较廉价的信息渠道获得与昂贵的单一信息渠道同一甚至更好的信息，如可用多个较为廉价的传感器获得与昂贵的单一传感器同一甚至更好的效果，因此可大大降低系统的成本。

概括地说，多源信息融合可以获得有关对象的更准确、更全面的信息；可明显抑制噪声，降低不确定性；可以弥补单一信息源的不准确性和测量范围的局限性；可以增加系统的可靠性。当某个或某几个传感器失效时，系统仍能正常运行，扩展了空间覆盖范围，扩展了时间覆盖范围，提高了空间分辨率，增加了测量空间维数。

随着自动化技术在各个领域的深入渗透，有效地运用传感器所提供的信息进行信号的综合处理，提高系统的性能，满足系统完成各种复杂任务的需要，显得愈来愈重要。尤其在智能系统中，要求系统能快速地获取周围环境的信息，对这些信息进行解释和处理，并能在未知环境中工作。但是目前靠单一的信息源很难满足准确获取环境信息的快速性和准确性的要求，会给系统对周围环境的理解及系统的决策带来影响。因此，需要有效地处理各种各样的大量多源信息，处理这些信息意味着加大了待处理的信息量，很可能会涉及在多源数据之间的数据矛盾和不协调，根据人的信息融合原理，我们知道最重要的是要开发一种消除这种矛盾和不协调的技术即信息融合技术。当采用多源信息融合技术后，能利用各种信息源在性能上的差异和互补性弥补单一信息源的缺陷，融合来自各种信息源的信息，综合分析而得到对周围环境的正确理解的稳定可靠信息，使系统具有容错性，提高系统信息处理的速度和决策的正确性。当信息处理技术从单个信息源演变成多个信息源处理时，信息源技术也需要演变为分布式并行处理，信息源之间的网络结构形成了这种发展趋势的基础，最重要的是对多源信息融合方法进行改进，以使为改进这些信息源网络的不协调性提供方法。

单一信息源获得的仅是环境特征的局部，片面的信息，它的信息量是十分有限的。而且每个信息源还受到自身品质、性能噪声的影响，采集到的信息往往是不完整的，带有较大的不确定性，甚至偶尔是错误的。因此，对大量不同来源的信息进行融合与智能处理是必要的。各种信息源的特点表明，信息融合并不是很简单的事情，由于信息源数据的不准确、延迟、虚警等，会将错误的信息包含进去。因此，要通过信息融合去伪存真，由此及彼，由表及里，将各种信息源中有用的信息挑出来，汇集成全面的、深刻的、立体的信息。

9.1.2　信息融合的发展历史

多源信息融合技术萌芽于第二次世界大战中对飞机、轮船、潜艇和 V—1 导弹的导航制导，当时叫做组合导弹制导，20 世纪 80 年代多源信息融合技术才开始进入应用研究阶段。在公开的技术文献中，多源信息融合概念最早是由 Tenney 和 Sandell 在 70 年代末期提出的，当时并未引起人们足够的重视，随着科学技术的迅猛发展，军事和工业领域中不断增长的复杂度使得军事指挥人员或工业控制环境面临数据瓶颈和信息超载的问题，需要新的技术途径对过多的信息进行消化、解释和评估，人们越来越认识到信息融合的重要性。在世界上几次局部战争中，信息融合显示了强大的威力，特别是在海湾战争中，多国部队的 C^3I（Command，Control，Communication and Intelligence）系统发挥的作用已引起了全世界的普遍关注，由于信息融合系统本身所具有的良好的鲁棒性、宽阔的时空覆盖区域、高维的测量和良好的目标空间分辨率，以及较强的故障容错与系统重构能力等潜在的特点，西方各国的国防部门都将其列为军事高科技研究和发展领域中的一项重要专题。美国国防部早在 1984 年就成立了数据融合专家组，指导、组织并协调有关这一国防关键技术的系统性研究，从而在 80 年代中期，信息融合技术首先在军事领域研究中取得了突破性的进展。由于信息融合的早期研究大多着重于增强计算能力和有效组织数据的具体方法，并且这些研究主要是基于军事应用背景的，所以在长时期内其技术一直是处于封闭状态。随着研究的深入和应用领域的扩大，有关这方面研究内容及成果才逐渐大量披露于各种学术会议和公开文献中。

9.1.3　信息融合的研究现状

1．国外研究现状[3,4]

国外对信息融合技术的研究起步较早，从 1973 年就开始迅速发展。1985 年以来，先后出版了 10 余部有关信息融合方法的专著。美国是信息融合技术起步最早、发展最快的国家。1984 年成立了信息融合专家组。美国国防部自从在海湾战争实际体会到了信息融合技术的巨大潜力后，更加重视信息自动综合处理的研究，在 C^3I 中增加了计算机，建立了以信息融合为核心的 C^4I（Command，Control，Communication，Computer and Intelligence）。除美国外，其他西方国家也普遍重视信息融合技术的研究。英国陆军开发了诸如炮兵智能信息融合系统（AIDD）、机动和控制系统（WAVELL）等，并于 1982 年提出了研制“海军知识库作战指挥系统”；1987 年又与西德等欧洲五国制订了联合开展“具有决策控制的多传感器信号与知识综合系统（SKIDS）”的研究计划。1988 年，美国国防部把信息融合列为 20 世纪 90 年代重

点发展研究开发的二十项关键技术之一，且列为最优先发展的 A 类。资料表明，信息融合技术研究成果以美国最多，除涉及秘密外，主要公开发表在美国的三军信息融合年会、SPIE 传感器融合年会、国际机器人及自动化会刊、IEEE 有关系统、人和控制会刊等。为了进行广泛的国际交流，1998 年成立了国际信息融合学会（International Society of Information Fusion，ISIF），每年举行一次信息融合国际学术大会，总部设在美国。

在十几年的研究中，人们对信息融合的方式、系统的结构、融合系统中的信息表示与转换等问题做了一些研究，总的来说，可以归纳为以下几个方面。

（1）信息融合的层次：决定对多源信息在哪一阶段进行何种处理，融合层次的决定关系到信息的处理量、信息的抽象性、决策的正确性及系统的容错性。

（2）信息的表示和转换：将不同的信息源转换成为统一的表示形式，有效地实现各种信息源之间的比较、通信，便于信息的融合。

（3）信息融合的结构：根据信息的性质、对象的特点和系统的要求，对多源信息进行控制和管理，选择合适的融合结构。

（4）信息融合的方法：决定对多源信息进行各种综合分析和处理，并进行推理，得出对对象准确可靠的理解。

大多数信息融合系统使用了不同类型的传感器，但并没有把这些传感器看做一个整体来分析，虽然在传感器信息处理与分析方面已开展了大量富有成果的研究工作，但由于忽视了多传感器融合的研究，这无疑对提高各种智能系统的性能带来了不利的影响。人们不得不遗憾地承认，目前世界上智能最强的智能系统适应环境变化的能力还十分有限，远远达不到人们预期的目标，现有的智能系统基本上只能在环境的不确定性很小的结构化或半结构化条件下工作。虽然信息融合的应用研究已是如此广泛，但是信息融合本身却至今仍未形成基本的理论框架和有效的广义融合模型及算法。其绝大部分工作是针对特定应用领域内的问题开展研究的，也就是说，目前对信息融合问题的研究都是根据问题的种类，各自建立直观融合准则，并在此基础上形成广泛的所谓最佳融合方案。这些研究反映的只是信息融合所固有的面向对象的特点，也就难以构成信息融合这一独立学科所必需的完整理论体系。这一理论短缺现象阻碍了研究者对信息融合本身的深入认识，也使得信息融合在某种程度上仅被看成是一种多传感器信息处理概念；人们很难对融合系统做出综合分析与评估，使得融合系统的设计带有一定的盲目性。因此，即使有不少学者曾探索了融合系统的性能评估问题，但这类评估大多只是提出一些特定的系统性能指标，或者针对特定的应用背景来对某种融合算法进行分析。

在信息融合领域，理论研究远远落后于实际需要，至今尚未形成具有普遍指导意义下的较为严格的原理和方法。多源信息融合技术还是一门很不成熟的技术，目前对信息融合过程本身的功能与形式也还没有一个统一的定义，还不能对一般信息融合建立通用的数学模型，目前的信息融合实用系统大多以专家系统设计方法为实现基础，专门用于多传感器信息融合

问题的通用结构设计的基础研究已经开始，但还没有突破性的实质进展。关于信息融合的研究内容和方法，有各种不同的说法。有人从数学和控制的角度将信息融合解释为多元信息的最优估计，有人则认为不能简单地将信息融合看做是一件事或一项技术，而应当看做是一种智能思维方式。尽管看法各异，但人们共同的认识是：在一般情况下，使用多个信息源比只使用单一信息源能够获得更准确、更全面、更可靠的环境信息，关于这一点，Richardson 给出了理论上的证明。

在信息融合处理前，必须对信息进行关联，以保证所融合的信息是有关同一目标或现象的信息，即保证信息的一致性。如果不同目标或现象的信息进入融合系统，将难以使得系统得出正确结论，这一问题称为关联的二义性，是信息融合所要克服的主要障碍，由于在多传感器信息融合中引起信息关联的二义性很多，如传感器测量的不精确性，干扰等，因此怎样确立信息可融合性的判断准则，如何进一步降低关联的二义性，已成为信息融合研究亟待解决的问题，另外系统的容错性或鲁棒性，也是信息融合理论研究中所必须考虑的问题。

少数已建成的信息融合系统仅仅是以一种简单的方式合成信息，还没有充分有效地利用多传感器所提供的冗余信息，而且许多工作仍处于探索或仿真阶段。在信息融合系统设计方面也还面临许多实际问题，如传感器测量误差模型的建立、复杂动态环境下系统的实时响应、大知识库的建立及其管理等。

2．国内研究现状[4,5]

国内信息融合技术研究起步较晚，基本处于搜集、吸收和跟踪国外先进技术的阶段。在我国由于缺乏实际的多传感器应用需求的牵引，使多传感器信息融合的研究具有探索性和预研性，尽管有许多的研究者，但还没有相应的学术团体，没有学术交流的机会和专刊，信息融合这一术语尽管被广泛地使用，其研究也得到了政府和个别基金部门的大量资助，引起众多研究者的极大兴趣，但它的含义却有不同的解释，经常被错误地理解，这导致了我国在信息融合领域的研究进展缓慢，甚至对于信息融合的概念及其从基础理论到实际应用研究的主要内容、要解决的关键问题和当前面临的主要问题还缺乏一个基本的了解。

对信息融合基础理论、综合利用人工智能、神经网络、并行处理机制、专家系统及军用机器人等项目的研究正在起步，中国舰船研究院开发了针对海军舰艇的试验系统，在国内较早地进行了信息融合的探索研究。航天二院二部与空五所、二十三所联合进行了制导雷达组网试验，在信息融合技术研究中取得了较丰富的经验。

从已发表的公开文献来看，从 1988 年开始有关信息融合的文章才陆续多起来，而且这些文章基本上是有关综述、译文和理论推导，实际应用者较少，更未见到实际成功应用的例子。1995 年，由国防科工委组织的 20 多位代表在长沙召开了第一次信息融合研讨会，从会上交流的学术论文来看，我国多源信息融合的研究还处于初级阶段。

随着国外信息融合技术研究的发展和计算机数据存储能力的大幅度提高，近几年我国对于信息融合方面的研究日益重视。例如，国家自然科学基金资助的北京航空航天大学的“多传感器信息融合”项目，电子工业部在成都电子科技大学的预研项目，总装备部和国防科工委对部队院所的多传感器信息融合研究也进行了资助。也有一批高等院校和研究所展开了该领域的研究，如四川大学研制的多航管雷达信息融合系统，该系统性能达到了世界领先水平，且已经实地运行在广州白云、深圳、成都双流等多家航空港。中科院遥感所开发的图像信息融合软件已成功地应用在卫星地面站的图像分类与识别中。

由于大批院校和研究所的技术投入，国内有关信息融合的研究取得了许多成果。但是，这些成果大部分集中在思想体系和各种算法上，处于起步阶段，离实际工程应用尚远。20 世纪 90 年代中期，信息融合技术在国内已发展成为多方关注的共性关键技术，出现了许多热门的研究方向，许多学者致力于机动目标跟踪、分布检测融合、多传感器综合跟踪与定位、分布信息融合、目标识别与决策信息融合、态势估计与威胁估计等领域的理论及应用研究，相继出现了一批多目标跟踪系统和有初步综合能力的多传感器信息融合系统。值得注意的是，多源信息融合的研究已经引起了国家有关部门的高度重视，并列入“863”计划，1997 年，国家自然科学基金把信息融合技术作为鼓励研究领域重点推出。

9.1.4 信息融合的发展趋势

随着科学技术的发展，新型敏感材料和传感器不断涌现，传感器种类的增多、性能的提高及精巧的结构都促进了多传感器信息融合的发展。多传感器系统所采集的信息量将大大增加，而这些信息在时间、空间、可信度、表达方式上不尽相同，侧重点和用途也不同，这对信息的处理和管理工作提出了新的要求。若对各种不同传感器采集的信息进行单独、孤立地加工，不仅会导致信息处理工作量的增加，而且割断了各种传感器信息间的内在联系，丢失了信息有机组合可能蕴涵的对象特征，从而造成信息资源的浪费。另外，由于传感器感知的是同一环境下不同（或相同）侧面的有关信息，所以这些信息的相关是必然的，由此，多传感器系统要求采用与之相应的信息综合处理技术，协调各传感器彼此间的工作，传感器信息融合的有关理论，就是为了更有效地处理多传感器系统的各种信息而发展起来的一个新的研究方向。虽然当今的信息技术已经给人们带来了不曾奢望的利益，但技术前进的脚步是不会停止的，在面向 21 世纪的信息技术变革中，信息技术的发展方向将是智能化，智能信息处理是集系统内、外部各种信息形式，利用某种关于信息的经验和知识，在以算法为核心的传统信息处理技术的基础上，将启发式知识获取及上下层知识处理相结合的信息处理技术。它有望解决信息量不完全而导致系统的病态问题，用数学模型难以描述的非线性和不确定性问题，以及计算复杂性和实时性问题。当前多源信息融合发展趋势主要集中在[3~5]以下几个方面：

（1）建立信息融合的基本理论，编撰信息融合词典，规范领域术语和定义。

（2）兼有鲁棒性和准确性的融合算法研究。

（3）大系统中的融合技术，如算法分类和层次划分问题。

（4）发展并完善 JDL 模型，以解决现有 JDL 模型所不能处理的非军事问题。

（5）信息融合中的数据库和知识库技术的研究。针对具体应用问题，建立信息融合中的数据库和知识库，研究高速并行推理机制，是信息融合技术工程化及实际应用中的关键问题，是未来的研究重点之一。

（6）建立系统设计的工程指导方针，研究信息融合系统的工程实现。信息融合系统是一个具有强烈不确定性的复杂大系统，如何根据现有理论、技术、设备，保证金融系统的精确性、实时性及低成本是未来研究的重点之一。

（7）建立信息融合系统的设计和评估方法。在评价信息融合系统性能时，不仅要分析和测试它们的功能和性能，还要把这种评价工作与所花费的成本和实施的难易程度、现实性联系起来，因而必须首先建立合理的评价指标。作为融合系统性能的评价工具，需要广泛开发大规模计算机模拟技术和融合算法测试试验床技术。

（8）应用领域的扩展。现有资料表明，信息融合已经成为智能信息处理的一种通用工具和思维模式，除了目前在军事、医学、地理科学、机器人、工程等广泛应用外，在包括现代制造领域、农业应用领域、经济商业领域等其他领域的应用是信息融合的一个重要发展趋势。

（9）交叉学科的交流是未来信息融合技术研究的热点。作为现代信息技术与多学科交叉、综合、延拓产生的新的系统科学研究方向，信息处理及人工智能等领域的很多新技术都可以借鉴到信息融合的研究领域。多传感器系统反映的信息既有全面又有局部特征，神经网络会在目标识别和鲁棒多传感器系统两个领域里发挥重要作用。如何利用集成的智能计算方法（如模糊逻辑与神经网络的结合、模糊逻辑与进化计算的结合、神经网络与进化计算的结合等）提高融合系统的性能是值得深入研究的问题。人工智能和神经网络方法将继续成为信息融合研究的热点。

9.2　信息融合技术基础

9.2.1　信息融合的基本原理[1,2]

多传感器信息融合是人类和其他生物系统中普遍存在的一种基本功能。人类本能地具有将人体各种功能器官（眼、耳、鼻、四肢）所探测到的信息（景物、声音、气味和触觉）与

先验知识进行综合的能力，以便对周围的环境和正在发生的事件做出估计。这一处理过程是复杂的，也是自适应的，它将各种信息（图像、声音、气味、物理形状、描述）转化为对环境的有价值的解释，这需要大量不同的智能处理，以及适用于解释组合信息含义的知识库，也称为先验知识。因此，人的先验知识越丰富，综合信息处理能力越强。

一个智能化的检测系统要想获得对周围环境的认识，必须应用传感器技术。因此，传感器是智能系统感知外部世界信息的“感官”，具有信息融合能力的智能系统，是对人类高智能信息处理能力的一种模仿。

多传感器信息融合实际上是对人脑综合处理复杂问题的一种功能模拟。在多传感器系统中，各种传感器提供的信息可能具有不同的特征：时变的或非时变的，实时的或非实时的，快变的或缓变的，模糊的或确定的，完整的或不完整的，可靠的或非可靠的，相互支持的或互补的，相互矛盾的或冲突的。多传感器信息融合的基本原理就像人脑综合处理信息的过程一样，它充分利用多个传感器资源，通过对这些传感器及其观测信息的合理支配和使用，把多个传感器在时间或空间上的冗余或互补信息依据某种准则来进行组合，以获得被测对象的一致性解释或描述，使该信息系统由此而获得比它的各组成部分的子集所构成的系统更优越的性能。

多传感器信息融合与经典信号处理方法之间存在本质的区别，其关键在于信息融合所处理的多传感器信息具有更复杂的形式，而且可以在不同的信息层次上出现。这些信息表征层次包括数据层（即像素层）、特征层和决策层（即证据层）。

单传感器信号处理或低层次的多传感器数据处理都是对人脑信息处理过程的一种低水平模仿，而多传感器数据融合系统则是通过有效地利用多传感器资源，来大幅度地获取被探测目标和环境的信息量。

多传感器信息融合不仅是一个信息处理的理论概念，同时也是一个系统概念。无论是单层融合还是多层融合，多传感器信息融合系统都必须具有以下主要模块：

（1）对于特定的应用采用何种算法和技术以达到最优化；

（2）采用何种结构（即信息在何处融合）；

（3）怎样处理单个传感器以提取最大的信息量；

（4）采取何种精度进行信息融合；

（5）在动态环境下如何实现融合过程的最优化；

（6）数据采集环境如何影响处理过程；

（7）在何种情况下多传感器信息融合能提高系统性能；

（8）传感器信息的协调管理（即实现数据配准和关联）。

9.2.2　信息融合的功能模型

多源信息融合系统的设计，目前还没有一个统一的模式，还找不到一个行之有效的方法。综合众多的研究文献，作者认为信息融合模型主要包括信息融合的功能模型、结构模型和数学模型。功能模型是从融合的过程出发，描写信息融合包含哪些功能、数据库，以及进行信息融合时系统各组成部分之间的相互作用过程；结构模型从融合组成出发，说明信息融合系统的结构；数学模型则是信息融合算法和综合逻辑。这 3 大模型是任何一个融合系统都必须解决的，因此它们构成了融合系统的核心问题。本章将详细阐述融合系统的功能模型、数学模型和结构模型及信息融合的层次。目前的信息融合实用系统大多以专家系统设计方法为实现基础，专门用于信息融合系统设计的基础研究已经开始，但还没有取得突破性的实质进展。虽然信息融合的应用研究已十分广泛，但绝大部分的信息融合工作都是针对特定应用领域内的问题来展开的，即根据问题的种类，各自建立直观的融合准则，选取相应的融合算法。由于很多研究成果并不能推而广之，因此难以构成信息融合这一独立学科所必需的完整理论体系。此外，由于缺乏公共的参考框架，人们也很难对融合系统做出综合分析与评估，这就使得融合系统的设计带有一定的盲目性。

因此，众多学者一直致力于信息融合的基础理论研究，积极探讨信息融合系统的功能要素，以及这些要素组成信息融合系统的方式和规律，希望构建出信息融合的一般功能模型，为信息融合理论的研究者提供公共参考框架。

实用的信息融合系统应该具备以下功能：

（1）信息采集功能，负责向系统提供原始观测信息；

（2）信息的特征提取、分析功能；

（3）识别、跟踪、评估等功能；

（4）决策功能;

（5）系统的输出与响应功能;

（6）数据库、知识库的支持与管理功能;

（7）信息采集的控制与管理功能。

对于信息融合系统来讲，信息采集模块的控制与管理是必不可少的环节。所以，实际系统中需要构造闭环系统，从而可以根据信息融合的决策结果实现对信息采集模块的控制与管理。

很多学者如 Edward waltz、James Linas 等人很长时间以来一直致力于信息融合的基础理论研究，积极探讨信息融合系统的基本组成要素，并极力弄清这些要素组成信息融合系统的方式和有关规律，以建立不同类型信息融合过程的统一标准和模式，用统一的术语和度量标

准来解释基础过程，因此开发一个信息融合系统的一般功能模型，为信息融合的研究者提供一个参考框架就显得越来越重要。

形成详细合理的功能模型是信息融合学科走向成熟的一个重要标志，这样的模型可以为重要的通信载体服务，人们可以通过通信载体来探讨和评估模型的设计概念、算法和工作策略，这些模型也可以辅助信息融合中共性的东西发展成为公共的功能模块或处理标准。已有很多学者从不同的角度提出了融合系统的一般功能模型，其中最有代表性的功能模型有美国联合管理局信息融合研究小组提出的 JDL 模型、瀑布模型、Omnibus 模型、FH 模型等。

1．JDL 模型

JDL 模型由对象评估、势态评估、威胁评估和过程评估四级组成，第一级对象评估是结合位置信息、参数信息和身份信息来实现个体的严密表达，它主要完成四个关键功能：

（1）传感器数据的单位和坐标的一致转换；

（2）物体位置、运动特性和属性的实时估计；

（3）分配数据级对象允许静态统计技术的应用；

（4）物体识别和分类。

第二级势态评估用来描述环境中物体之间的当前关系，聚类分散的单个物体，它重点强调物体之间的关系信息。第三级威胁评估主要用于军事上，它根据敌方兵力和意向估计自己兵力的强弱。过程评估可以看成一个中间过程，主要完成四个关键作用：

（1）控制融合过程的性能，提供实时控制的信息；

（2）鉴别什么样的信息能改善融合的结果；

（3）搜集相关信息，决定信息源的具体要求；

（4）分配和指导信息源以达到某一目标。

功能模型中的第一级又可以分成不同的子集，一至四级的划分是人为的划分，实际的信息融合系统是这几个部分的集成和交叉。JDL 模型起初是为军事领域而建立的，它同样可以用到非军事领域。目前，信息融合的大部分工作集中在第一级上。

JDL 模型已成为研究信息融合的基本出发点，将信息融合分为四个级别，确定了处理流程中人为的逻辑分割，这些级的建立，也部分地得到了有关数据处理过程的共同术语，该模型强调信息产品，即数据融合处理中的各个步骤，而不强调计算机上的结构形式。当处理从第一级移到第三级时，该模型也强调推理层次，经过这些层次，融合产品的大部分将从很特殊的情况推广到较一般的情况。

由于信息融合是对多源信息进行阶梯状的、多层次的处理过程，该系统所实施的第一个融合过程，在其每一个环节上，各种数据所携带的有用的信息量都应发挥到最大的程度，使得融合结果对系统用户有利；而且，每一数据所携带的有用信息量在其所处的局部过程中所

起的作用，应该与其他部分的作用有机地连接在一起，以至于当一个局部过程十分紧密地接近感觉经验时，由此产生的有效信息的作用不至于在进入系统的其他过程时被减弱，即系统的各个部分达到了和谐与统一。

JDL 模型强调的是信息融合的推理层次而非计算机上的结构形式，因此，该模型并没有指明信息在整个系统中的流向，而人们在设计信息融合系统时通常希望能够对信息的流动加以控制。此外，与瀑布模型类似，JDL 模型也没有反馈机制。

2．瀑布模型（Waterfall Model）[6]

M．Bedworth 等人于 1994 年提出瀑布模型，如图 9.1 所示，广泛应用于英国国防信息融合系统，并得到了英国政府科技远期规划数据融合工作组的认可。瀑布模型将大量的数据经过信号采集、预处理、特征提取、模式匹配等环节后逐步提炼，直至到达瀑布的顶部，也就是决策环节。它重点强调了较低级别的处理功能。它的信号获取和处理、特征提取和模式处理环节相对应于 JDL 模型的第一级处理，而态势评估和决策制定分别对应于 JDL 模型的第二、三和四级处理。可以看出，尽管瀑布模型的融合过程划分得最为详细，但是它并没有明确的反馈过程，决策后获得的新信息也不能有效地运用于其他环节，这是瀑布模型的主要缺点。

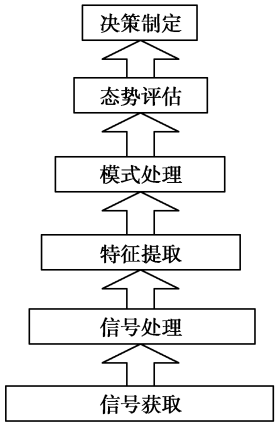


图 9.1　瀑布模型 [6]

3．Omnibus 模型

Gainey 和 Blasch 提出包含预测（Predict）、提取（Extract）、匹配（Match）、搜索（Search）等 4 个处理模块的 PEMS 控制回路，类似的结构还有 Boyd 提出的观测、定向、决策、控制环路（Boyd Control Loop）和英国智能协会提出的收集、核对、评估、情报循环（Intelligence Cycle）。

Bedworth 在对多种模型进行对比分析后提出了 Omnibus 模型。该模型综合了各模型的优点，利用 Boyd 回路控制信息流动，采用瀑布模型对数据融合中各处理过程的定义，同时借鉴 JDL 模型对信息融合功能的分级结构，使模型更适应具有复杂决策要求的应用领域。该模型保留了 Boyd 控制回路结构，从而明确了信息融合处理中的循环特性，模型中四个主要处理任务的描述取得了较好的重现精度。另外，在模型中也较为容易地查找融合行为的发生位置。Omnibus 模型是在瀑布模型的基础上加以改进的，增加了决策响应和信息反馈过程，在 Omnibus 模型中可以很清楚地看到反馈。遗憾的是，Omnibus 模型没有考虑到知识库和系统数据的管理需求，而实用的信息融合系统往往离不开数据库和知识库的支持。

4．FH 模型[7]

既然信息融合的功能结构和信息融合的层次结构都是信息融合系统的核心问题，那么，在设计信息融合的功能模型时兼顾到信息融合的层次不仅有助于提高信息融合系统的灵活性和普适性，也更有利于模式的统一。图 9.2 是结合信息融合的功能结构和层次结构提出的多模态信息融合的一般功能模型，简称为 FH（Function & Hierarchy Framework）模型，模型描述如下。

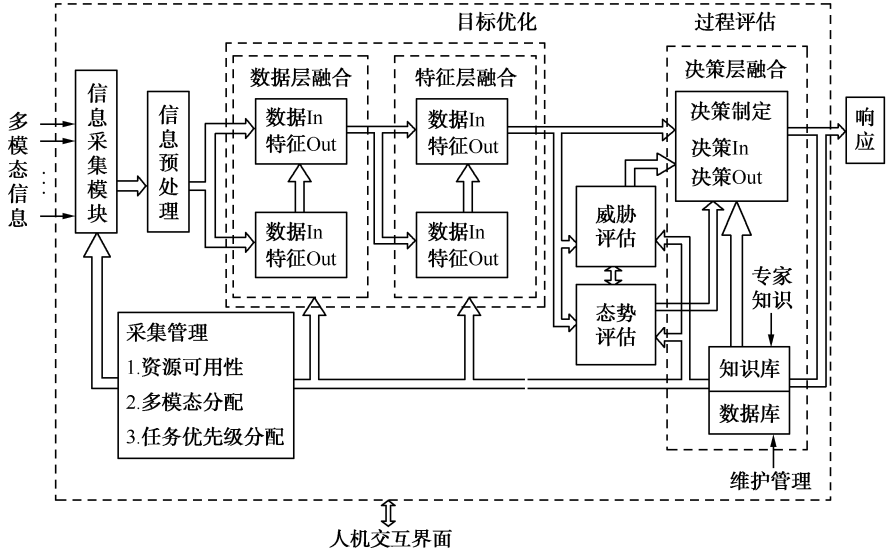


图 9.2　多模态信息融合的一般功能模型[7]

信息预处理：包括状态检测、坐标转换、单位换算、数据相关、轨迹估计，其目的是对采集的数据进行一致性检验、归一化等处理。

目标优化：目标优化是由数据层融合和特征层融合组成的，其任务是对各模态所获得的状态及属性的估计进行融合，实现对目标位置、运动特性及目标属性的实时估计。数据层融合可分为两类：数据输入→数据输出，数据输入→特征输出。相应地，特征层融合也可以分为特征输入→特征输出和特征输入→决策输出两类。

态势评估、威胁评估：属于高层的信息融合模式，主要用于军事领域，其目的是根据获取的信息进行事件预测，必要时发出威胁警告。如果用于非军事领域，则可以用态势评估来描述环境中各物体之间、物体与环境之间的关系。

过程评估：结合知识库和数据库信息评估融合过程的性能，鉴别什么样的信息可以改善

融合的结果，并搜集相关信息，分配和指导各环节以完成系统任务。

采集管理：用于管理系统资源，根据过程评估的结果重新分配任务优先级和各模态的工作。

数据库和知识库管理：定量地描述各模态的特性，以及各种外界条件对各模态特性的影响。分为实时数据库、非实时数据库、专家知识库等，实时数据库用于向系统提供当前观测结果及融合所需要的各种其他数据，并存储中间结果；非实时数据库存储历史数据及有关环境和目标的辅助信息。数据库要求容量大、搜索快、开放互联性好。知识库用来存储专家知识，是由事实性知识和推理性知识组成的，包含描述关系、现象和方法的规则，以及在系统专家范围内解决问题的知识。

9.2.3　信息融合的层次结构

多传感器信息融合与经典信号处理方法之间存在本质的区别，其关键在于信息融合所处理的多传感器信息具有更复杂的形式，而且可以在不同的信息层次上出现。按照融合过程中信息抽象的层次，可以将信息融合过程分为三个层次，即数据层（Data Level）融合、特征层（Feature Level）融合和决策层（Decision Level）融合。

1．数据层融合

数据层融合也称为像素层融合，它是直接在采集到的原始数据层上进行的融合，在各种传感器的原始测报未经预处理之前就进行数据的综合与分析。数据层融合一般采用集中式融合体系进行融合处理过程。这是低层次融合，如成像传感器中通过对包含若干像素的模糊图像处理来确认目标属性的过程就属于数据层融合。

数据层融合的主要优点是能保持尽可能多的现场数据，提供其他融合层次所不能提供的细微信息，但局限性也是很明显的。

（1）它所要处理的传感器数据量太大，故处理代价高，处理时间长，实时性差。

（2）这种融合是在信息的最低层次进行的，传感器原始信息的不确定性、不完全性和不稳定性要求在融合时有较高的纠错能力。

（3）进行图像融合时，要求各传感器信息之间具有精确到一个像素的校准精度，故要求各传感器信息来自同质传感器。

（4）数据信息量较大，抗干扰能力较差。

数据层融合通常用于多元图像复合、图像分析与理解、同类（同质）雷达波形的直接合成等。多元图像复合是将不同传感器获得的同一景物的图像经配准、重采样和合成等处理后，获得一幅合成图像的技术，以克服各单一传感器图像在几何、光谱和空间分辨率等方面存在

的局限性和差异性，提高图像质量。图像分析与理解主要研究利用高分辨率扫描传感器的输出，演绎出所观察情形的三维模型问题。数据层的融合技术包括经典的检测和估计方法。

从信息融合的角度来看，由于没有任何办法对原始数据所包含的特性进行一致性检验，数据层的融合具有很大的盲目性，因而一般不会直接在数据层进行融合过程，但由于图像处理本身的特殊性，才保留了数据层这一带有浓厚图像处理色彩的融合层次。多元图像融合的一个难点是中间图像的配准（Interimage Co-registration）。这一问题要求两幅或多幅图像之间配准以确保叠加的每幅图像上相应的像素代表同一位置。由于图像传感器是非线性的，而且在被观测的 3D 空间和 2D 空间图像平面之间要执行一个复杂的变换，这使得配准更加恶化。

2．特征层融合

特征层属于中间层次的融合，它先对来自传感器的原始信息进行特征提取（特征可以是目标的边缘、方向、速度等），然后对特征信息进行综合分析和处理。特征层融合的优点在于实现了可观的信息压缩，有利于实时处理，并且由于所提取的特征直接和决策分析有关，因而融合结果能最大限度地给出决策分析所需要的特征信息。特征层融合一般采用分布式或集中式的融合体系。

特征层融合可分为两大类：一类是目标状态融合，另一类是目标特性融合。

1）目标状态融合

目标状态融合主要应用于多传感器目标跟踪领域，目标跟踪领域的大量研究方法都可以修改为多传感器目标跟踪方法。图 9.3 说明了特征层目标状态信息融合的基本内容。融合系统首先对传感器数据进行预处理以完成数据配准。在数据配准后，融合系统主要实现参数关联和状态矢量估计。

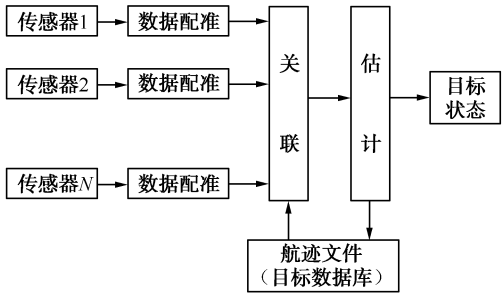


图 9.3　特征层目标状态信息融合的基本内容

参数关联把来自多传感器的观测与传感器各自的观察对象联系起来，各传感器观察分别组合在一起以保证这些观察分别属于各自的观察对象，一旦关于同一对象的各个观察相互关

联后，就可以应用估计技术来融合这些关联后的数据，以得到估计问题的解。由于计算上的好处，常采用序贯估计技术，其中包括卡尔曼滤波和扩展卡尔曼滤波。

目前该领域的发展所遇到的核心问题是如何针对复杂环境来建立具有良好稳健性及自适应能力的目标机动和环境模型，以及如何有效地控制和降低数据关联即递推估计的计算复杂性。

2）目标特性融合

特征层目标特性融合就是特征层联合识别，它实质上是模式识别问题。多传感器系统为识别提供了比单传感器更多的有关目标的特征信息，增大了特征空间维数。具体的融合方法仍是模式识别的相应技术，只是在融合前必须先对特征进行关联处理，把特征矢量分类成有意义的组合，特征层目标特性融合的基本结构如图 9.4 所示。

对目标进行的特性融合识别，就是基于关联后的联合特征矢量进行模式识别。具体实现技术包括参数模板法、特征压缩和聚类算法、*K*-阶最近邻、人工神经网络、模糊积分等。除此之外，也采用基于知识（Knowledge-based）的推理技术进行特征层融合识别，但由于难以抽取环境和目标特征的先验知识，因而这方面的研究仍处于起步阶段，至今尚未看到系统化的结果。

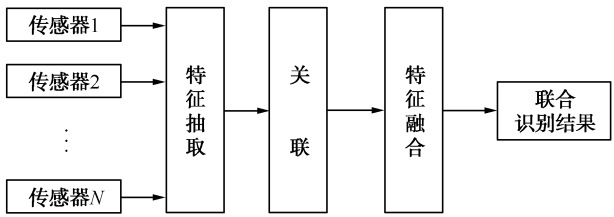


图 9.4　特征层目标特性融合的基本结构

3．决策层融合

决策层融合通过不同类型的传感器观测同一个目标，每个传感器在本地完成基本的处理，其中包括预处理、特征抽取、识别或判决，以建立对所观察目标的初步结论。然后通过关联处理进行决策层融合判决，最终获得联合推断结果。

从理论上来说，决策层联合输出的联合决策结果比任何单传感器决策更为精确或更为明确。但是除非各传感器的信号是相互独立的，否则决策层融合的分类性能可能低于特征层融合。决策层所采用的主要方法有贝叶斯推断、D-S 证据理论、模糊集理论、专家系统方法、人工神经网络等。另外，决策层融合还采用一些启发式的信息融合方法来进行仿人融合判决。

决策层融合的主要优点有：

（1）具有很高的灵活性；

（2）系统对信息传输宽带要求低；

（3）能有效地反映环境或目标各个侧面的不同信息类型；

（4）当一个或多个传感器出现错误时，通过适当的融合，系统还能获得正确的结果，所以具有容错性；

（5）通信量小，抗干扰能力强；

（6）对传感器的依赖性小，传感器可以是同质的，也可以是异质的；

（7）融合信息处理代价低。

目前有关信息融合的大量研究成果都是在决策层上取得的，并且构成了信息融合研究的一个热点。但出于环境和目标的时变动态特性、先验知识获取的困难、知识库的巨量特性、面向对象的系统设计要求等，决策层融合理论与技术的发展仍受到阻碍。

9.3 信息融合常用算法

9.3.1 加权融合算法

加权平均是一种最简单和直观的方法，即将多个传感器提供的冗余信息进行加权平均后作为融合值。该方法能实时处理动态的原始传感器读数，但调整和设定权系数的工作量很大，且具有一定的主观性。对加权系数法的改进，可以采用模糊贴近方法，常用的贴近度方法有：两模糊子集的内积（外积）、两模糊子集的距离（加权海明距离）、最大最小法、集函数法等。

仲崇权等人[8]将多传感器对某一状态的测量结果分组，针对每组测量变量的算术平均值，依据极大似然原理，提出了多传感器分组加权融合算法。通过对各组传感器测量值的方差进行估计，从而对每组传感器测量平均值的权值进行合理的分配，解决了在传感器和环境干扰未知情况下，加权融合算法中权系数如何确定的问题。

9.3.2 贝叶斯估计

贝叶斯估计方法用在多传感器信息融合时，先将多传感器提供的各种不确定性信息表示为概率。将相互独立的决策看做一个样本空间的划分，使用贝叶斯条件概率公式对它们进行处理，最后系统的决策可用某些规则给出，如取最大后验概率的决策作为系统的最终决策，但这种方法存在以下不足[9]：

（1）需要给出各传感器目标类别的先验概率，即需预先经过大量的实验得到各先验概率分布，这在很多实际的系统中是比较困难的，甚至是不可能的；

（2）要求各种可能的决策相互排斥；

（3）当可能的决策较多时，先、后验概率的计算将变得很复杂，影响实时性。

所以，用贝叶斯方法解决多传感器信息融合问题时有一定的局限性，但在一定场合下，仍不失为一种行之有效的方法。

多贝叶斯估计是 Durrant-Whyte 提出的一种数理统计多传感器信息融合方法。该方法将系统中的各传感器作为一个决策者队列，通过队列的一致性观察来描述环境。即将每个传感器当做一个贝叶斯估计器，将每个物体的关联概率分布组合为一个联合的后验概率分布函数，然后使这个联合后验概率分布的似然函数达到最大，提供多传感器信息的最终融合值。

9.3.3　D-S 证据理论[5]

证据组合理论是由 Dempster 首先提出来的，后来由 Shafer 加以扩充和发展，由于主观贝叶斯方法从数学上看是蕴涵于证据理论之中的，所以证据理论有时也称为广义概率论。

1．证据的不确定性

证据理论主要就是要建立如下的信任结构。

假设 $U=\{x_1,x_2,\cdots,x_n\}$ 是一个有限集合，m 是 U 子集的度量，它满足：

（1）对任意 $A\subset U, 0\leqslant m(A)\leqslant 1$；

（2）$m(\phi)=0$；

（3）$\sum_{A\subset U} m(A)=1$。

其中，m 称为基本概率指派函数，它是从 U 的普通子集到单位区间上的一个映射集合。

$$m: 2^U \rightarrow [0,1]$$

U 的任何一个子集 A，如果它满足 $m(A)>0$，则称这一子集 A 为焦点元素。Shafer 将焦点元素限制为普通子集。我们称 m 和它的值就是一个信任结构 。这样我们就可以采用信任结构来表示某个元素或子集的一个证据。信任函数 Bel 和似然函数 PI 在证据理论中起着重要的作用。信任函数定义为：

$$\text{Bel}: 2^U \rightarrow [0,1]$$

对任意 $B\subset U$，有

$$\text{Bel}(B)=\sum_{A\subset B} m(A)$$

似然函数定义为：

$$\mathrm{PI}: 2^U \to [0,1]$$

对任意 $B \subset U$，有

$$\mathrm{PI}(B) = \sum_{A \cap B \neq \phi} m(A)$$

其中，A，B 为 U 的子集；$\mathrm{Bel}(B)$ 度量分布在 B 的元素中的概率总值；$\mathrm{PI}(B)$ 度量分布在 B 的元素中的最大概率值。显然，Bel 和 PI 满足如下的关系：

$$\mathrm{PI}(B) > \mathrm{Bel}(B)$$

$$\mathrm{PI}(\phi) = \mathrm{Bel}(\phi)$$

$$\mathrm{PI}(U) = \mathrm{Bel}(U) = 1$$

$$\mathrm{PI}(B) = 1 - \mathrm{Bel}(\bar{B})$$

$$\mathrm{Bel}(B) + \mathrm{Bel}(\bar{B}) \leqslant 1$$

$$\mathrm{PI}(B) + \mathrm{PI}(\bar{B}) \geqslant 1$$

由于在证据理论中，缺少关于总概率的分配知识，所以不能确切地知道概率是如何分配给每个元素 $A \in U$ 的，因而也就不可能计算与 U 的子集有关的概率 $P(A)$，这样，就用 $\mathrm{Bel}(A)$ 和 $\mathrm{PI}(A)$来描述 A 的不确定性，它们相应于未知概率 $P(A)$的下界和上界，即：

$$\mathrm{Bel}(A) \leqslant P(A) \leqslant \mathrm{PI}(A)$$

证据理论不像概率论那样，必须求出先验概率，而且它把不知道和不确定区分开了。$\mathrm{PI}(A) - \mathrm{Bel}(A)$ 的值反映了对 A 的不知道的信息。

Halpern 总结了信任函数的两种解释。其一是源于 Dempster 的看法，认为信任函数是概率的下界，似然函数是概率的上界，由于证据理论也有类似于概率的三公理，从而有信任函数是概率函数的推广之说；其二是以 Smets 为代表的学者认为，信任函数只表示证据，和概率没有直接的联系。他们建立的可传递信任模型把推理过程分成两级：首先是信任级，它只考查证据影响信任的程度，不加主观判断；其次是决策级，利用不充分推理原则将信任函数转化为赌博概率进行决策。这样它与人的先思考再决策过程相符，显得较为客观。Yao 运用粗糙集理论解释了信任函数，为证据组合理论和粗糙集理论的发展奠定了基础。刘大有等人用布尔代数解释证据推理，推广了概率的上界和下界的含义。

2．证据组合理论的优缺点

证据组合理论的优点：

（1）理论基础较强，能处理由模糊性产生的不确定性；

（2）可以依靠证据的积累，不断地缩小假设集；

（3）能将不知道和不确定区别开来；

（4）如果条件满足，则信息和时间的复杂度可能很低。

证据组合理论的缺点：

（1）至今还没有研制出一个成功地应用 D-S 证据理论的知识系统，人们对 D-S 理论的不同解释可能得出不同的结果。

（2）除了很简单的情况外，D-S 组合规则真正的含义仍然不十分清楚，而且证据被分割开可能会导致一些错误的结果，此外，证据组合理论总假设证据是独立的，这也不是一个合理的假设。

（3）由 D-S 理论所计算出的结果在数值上有时缺乏稳定性，BPA 的一个很小的变化可能导致结果有较大的变化。而且当支持的证据不一致时，D-S 规则就无法使用。

（4）在推理链较长时，D-S 理论的使用就感到很不方便，这是因为在应用 D-S 理论时，必须首先把相应于每个推理步骤和证据的信任函数变换成一个一般的识别框架，然后才能应用 D-S 组合规则，当推理步骤增加时，由于最后结果的信任函数的焦点元素结构的复杂性也相应增加，所以 D-S 规则的递归应用就会感到十分困难。

（5）潜在的指数复杂度是使用困难的一个重要原因。

9.3.4　卡尔曼滤波

卡尔曼滤波用于实时融合动态的低层次冗余传感器数据，该方法用测量模型的统计特性递推决定统计意义下的最优融合数据估计。如果系统具有线性动力学模型，且系统噪声和传感器噪声是高斯分布的白噪声模型，卡尔曼滤波为融合数据提供唯一的统计意义下的最优融合数据估计，卡尔曼滤波的递推特性使系统数据处理不需要大量数据存储和计算。卡尔曼滤波有如下特点[10]：

（1）卡尔曼滤波处理的对象是随机信号；

（2）被处理信号无有用和干扰之分，滤波的目的是要估计出所有被处理的信号；

（3）系统的白噪声并不是需要滤除的对象，它们的统计特性正是估计过程中需要的信息。

所以确切地说，卡尔曼滤波应称为最优估计理论，此处所谓的滤波与常规滤波具有完全不同的概念和含义。利用卡尔曼滤波可将车辆的 GPS（全球定位系统）信息与 DR（车辆航位推算导航系统）信息进行融合，解决卫星信号丢失和航位推算误差随时间累积的问题。卡尔曼滤波也常将 GPS 与 INS（惯性导航系统）的信息进行融合，提高定位精度。卡尔曼滤波在机器人定位、车辆和舰船等定位方面应用得很广泛。

9.3.5 Markov 链[11]

基于 Markov 链的信息融合算法是利用 Markov 链组合多个传感器的观测值以形成一个一致的输出，并且这个输出是各个观测的线性加权组合。用自熵和条件熵分别来度量一个传感器对于自身观测值和共同观测值的确定性程度，以确定权值。

9.3.6 可能性理论[12]

在没有精确环境模型的情况下，使用可能性理论能比其他方法更适合于处理多传感器信息融合中的不确定性。可能性理论本质上更能反映实际被感知的对象和期望观测之间的相似性，实验结果表明，这种相似性和物体被观测到的次数并没有任何关系，这一点说明了概率理论的不足。

9.3.7 模糊逻辑[13]

在多传感器系统中，各信息源提供的环境信息都具有一定程度的不确定性，这些不确定信息和融合过程实质上是一个不确定性推理过程。模糊逻辑利用模糊子集 A 的隶属度可为[0,1]之间的任意值，允许将多传感器信息融合过程中的不确定性直接表示在推理过程中。如果采用某种系统化的方法对融合中的不确定性建模，则可产生一致性模糊推理。综合利用多传感器的信息来获得有关目标的知识，可以避免单一传感器的局限性，减小不确定性误差的影响。模糊推理在信息融合中常与其他方法一起使用，如模糊一致性推理、模糊神经网络等。

9.3.8 神经网络[14]

神经网络可根据当前系统所接收的样本的相似性确定分类标准。这种确定方法主要表现在网络权值分布上，同时可采用神经网络特定的学习算法来获取知识，得到不确定性推理机制。

基于神经网络的信息融合可分为 3 个重要步骤：

（1）根据系统要求和多传感器信息融合的形式，选择神经网络的拓扑结构；

（2）将各传感器的输入信息综合为一个总输入函数，并将此函数映射定义为相关单元的映射函数，它通过神经网络与环境的交互作用把环境的统计规律反映到网络本身的结构中；

（3）对传感器输出进行学习、理解、确定权值的分配，完成知识获取、信息融合，进而

对输入模式做出解释，将输入数据转换成高层逻辑概念。

基于神经网络的多传感器信息融合具有如下特点：

（1）具有统一的内部知识表示形式，通过学习算法可将网络获得的传感器信息进行融合，获得相应的网络参数，并且可将知识规则转换成数字形式，便于建立知识库；

（2）利用外部环境的信息，便于实现知识自动处理及并行推理；

（3）能将不确定环境的复杂关系，经过学习推理，融合为系统能够理解的准确信号；

（4）神经网络具有大规模并行处理信息的能力，使得系统信息处理速度很快。

9.3.9　粗糙集方法

粗糙集理论最早是由波兰数学家 Z.Pawlak 于 1982 年提出的，是一种处理模糊和不精确性问题的新型数学工具。他针对边界线区域思想提出了粗糙集，并把无法确认的个体都归属于边界线区域，而这种边界线区域被定义为上近似集和下近似集的差集。粗糙集理论在处理有限元集合时，通过对大量数据进行分析，根据论域中的两个等价关系的依赖关系，剔除相容信息，抽取潜在有价值的规则知识。其中，约简和核是两个重要的概念。

粗糙集理论在代数表示下，它的很多概念与运算的直观性较差，人们不容易理解其本质。另外，在代数表示下，目前还没有关于知识约简的高效算法，同一问题在不同知识表示下的算法难度是不同的。

基于粗糙集理论的信息融合的一般步骤为[15]：

（1）将采集到的样本信息按条件属性和结论属性编制一张信息表；

（2）利用属性化简及核等概念去掉冗余的条件属性及重复信息，得出简化信息表；

（3）求出核值表；

（4）由核值表求出信息表的简化形式；

（5）汇总对应的最小规则，得出最快融合算法。

9.4　信息融合的典型应用

信息融合的具体应用集中于军事领域和非军事领域，方便军事团体和非军事团体在应用领域进行技术交流。例如，由 IEEE 发起的第一届多传感器融合和混合的智能系统年会（The First International Conference on Multi-Sensor Fusion and Integration for Intelligent Systems）于 1994 年 10 月 2 日至 5 日在 Las Vegas，NV 举办。下面依次介绍信息融合在军事领域、人脸识别、语音处理与说话人识别，以及多生物特征认证中的应用。

9.4.1 军事中的应用[16]

军事团体的研究集中于对运动实体（如发射器、控制平台、武器和军队）的定位，特征提取和目标识别。军事领域相关应用的例子包括海洋监视系统，空对空防御系统，战场智能、监视和目标拦截系统以及战略警告和防御系统。

海洋监视系统用于探测、跟踪和辨识海上目标和事件，典型的应用包括支持海军舰队战略的反潜艇竞争系统和自动导航系统。传感器组包括雷达、声纳、电子情报（Electronic Intelligence）、通信量观测（Observation of Communication Traffic）、红外线和合成孔径雷达观测等。海洋监视系统所要面临的挑战是大容量的监视数据、目标和传感器的结合，以及复杂的信号传播环境（特别是水下声纳传感器）等。

空对空和地对空防御系统已经用于检测、跟踪、辨识飞机和防空武器。这些防御系统采用的传感器组包括雷达、无源电子支持测量（Passive Electronic Support Measures）、红外线、敌我辨识（Identification-Friend-Foe，IFF）传感器、光电图像传感器和可视观察等，用来支持争夺空中优势、飞机突袭、目标优先化和航线计划等多种活动。信息融合系统所要面对的挑战有敌方干扰、快速决策反应的需求，以及大量的目标参数传感器对（TargetSensor Pairings）的合成。敌我辨识系统所要面临的一个特别难题是如何准确地、没有任何差错地辨识敌机。全世界武器系统的快速增加，以及缺少武器来源和使用者之间的关系，都大大增加了 IFF 系统的难度。

另一个应用是战场智能、监视和目标拦截系统，用来检测和辨识潜在的地面目标。具体的例子有地雷的定位和高价值目标的自动识别。传感器包括移动目标显示（Moving Target Indicator）雷达、合成孔径雷达、无源电子支持测量、照片侦察、地下声学传感器、远距离领航飞机、光电传感器和红外传感器等。主要的推断是战场态势评估和威胁评估及航线估计。

为了满足军事应用的要求，在信息融合系统中需要采用以下一些措施来提高信息融合处理的自动化水平。

（1）使用多种传感器和多个频道（如无线电、红外、光电）的发射和反射，进行截获、检测、识别和跟踪目标。

（2）利用战区战术数据链和全球战略数据网在指挥和控制节点间有效地传输数据，交换互相关联的航迹和检测（事件），并进行传感器对传感器的交接。

（3）使用带有数据链的分布式传感器网络，提供具有改进检测和对抗性能的协调监视和定位能力。

（4）使用多个互补的无源传感器（如 ESM、IR 或 EO）发展无源的、低可观测性的武器系统，来替代或支持如雷达之类的单一、有源传感器系统。

信息融合军事应用的详细讨论可参阅 Proceedings of the Data Fusion Systems Conference，Proceedings of the National Symposium on Sensor Fusion 及相关的军方文件。

9.4.2　人脸识别中的应用

通过研究可以发现，对于复杂模式识别问题（如手写体汉字识别、人脸识别），可以说目前还没有一个简单的方法可以达到较高的识别率和可靠度，每一种方法都有各自的优点、缺陷和不同的适用范围，不同的特征和匹配方法之间具有一定的互补性。因此，研究如何将不同的方法有机地结合起来以充分发挥各自的优势，克服其缺陷，从而构成信息融合型的识别系统，就成为当前模式识别研究的一个主要方向。

实例 1：信息融合在人脸检测中的应用

1）人脸检测识别方法中的特征融合[17]

从不同的角度观察，人脸的特征是多种多样的，有肤色特征、轮廓特征（椭圆轮廓等）、启发式特征（头发、眼睛、下巴等）、模板特征（均值、方差、距离等）、变换域特征（特征脸、小波特征等）、结构特征（对称性、投影特征等）、镶嵌图特征（基于马赛克规则等）和直方图特征（分布、距离等）。

对称性是一种结构特征，是物体的基本性质之一，在计算机视觉研究中应用十分广泛，它包括点对称性（即中心对称性）和轴对称性，绝大多数自然物体都存在这两种对称性。对人脸这个特殊的物体来说，眼睛、眉毛、嘴巴等具有很强的点对称性，同时在姿态限制的情况下，上述人脸部件还具有很强的轴对称性。利用这种对称性的方法很多，如广义对称变换、方向对称变换、离散对称变换。上述方法在大范围尺度上实施时计算量很大，定位精确较差。

肤色特征是人脸的一个基本特征，在人脸跟踪、检测中已经得到广泛应用，肤色跟环境颜色的差异一般较大，分离性好，检测速度快。检测时要先建立彩色模型，然后建立人脸肤色模型，检测过程就是将待测颜色向肤色模型投影的过程，如果在肤色模型区域内，则认为是人脸的一部分。不过这种方法有一个很明显的缺陷就是不能将人脸与人的其他裸露部分区分开来，最常见的问题就是脖子与人脸的区分。

很直观的感觉，可以用其他的特征来协助肤色进行判断，于是就有了肤色结合对称性的检测方案构想，但是采取什么方式进行这种协助综合呢？有三种方法：

（1）先进行肤色区域分割，再对初选区域进行对称性分析判断；

（2）先进行对称性判断，再对初选区域使用肤色特征辅助判断；

（3）将肤色特征和对称性特征融合，利用新特征进行判断。

根据刚才的分析，前两种方法实质上是特征的串联工作，检测速度很慢，不能满足动态图像检测的速度要求，此处选用第三种方法并根据特点进行了进一步改进：

（1）利用肤色特征提取速度快的特点进行初选，得到待选小区域；

（2）基于一定的先验知识进行简单的归并，不进行大规模的颜色区域归并；

（3）利用镶嵌图的思想建立网格，对每个图像块按照规则进行计算统计，得到构造的肤色特征矢量和对称性矢量；

（4）按照线性加权法将两个特征矢量融合成一个特征矢量；

（5）利用新特征对待选小区域进行判断，得到检测结果。

改进方法中肤色特征和对称性特征的获取过程是基本同步的，而且融合特征的判断是在小的区域上进行的，使得该方法的检测速度大大提高。特征融合方法中的线性组合法因其计算量小、融合速度快和灵活性得到了广泛应用。

2）人脸检测识别方法中的决策融合

为了设计高性能的单分类器模式识别系统，一般的做法是首先提取模式的最优特征，然后设计最优的分类器。实际上要达到以上的两个最优是非常困难的。

对于复杂的模式识别问题，往往会遇到两个问题[18]：

（1）对于一个特定的模式通常有大量的、不同类型的特征可以用来表示和描述，这些特征的表示方式各不相同，可以是连续量、离散量或结构基元，其物理意义也是多种多样的，因而往往难以将它们合在一起用一个单独的分类器进行处理。

（2）在模式识别中，几乎每一个应用领域都存在着许多基于不同理论的分类方法，这些方法大体上可以归为统计方法和结构方法。更进一步，每类方法中又包括许多基于不同方法论的算法。例如，在统计方法中，就有线性分类器、最近邻分类器、各种距离分类器、人工神经网络分类器和支持向量机分类器（SVM）等。通常，对于一个复杂的应用问题，这些分类器中的任何一种都能取得一定的效果，但没有一种方法是完美无缺的。

第一个问题要求我们先采用不同的分类器处理不同的特征，再对各分类器的结果进行综合。第二个问题要求我们研究如何把众多不同分类算法集成起来，即把不同分类器的结果有效地综合起来得到更好的结果。实际上这两个问题就是决策融合问题（又叫多分类器融合、分类器集成、分类器组合等）。

一般认为，多分类器融合是设计一个高性能且稳定的人脸识别器的有效途径，不同性质的特征往往反映物体的不同方面，在一个特征空间很难区分的两种模式，可能在另一种特征空间上很容易分开；而对应于同一特征的不同分类器又从不同的角度（基于概率或最近距离等）将该特征映射到结果集合上。因此利用不同性质的特征和不同的分类器的融合就可能全面反映出一个物体，从而得到一个较好的分类结果。

3）基于投票法的决策融合应用实例[18]

设有 N 类模式 $X_n(n=1,2,\cdots,N)$，对于一个未知模式 x，使用 M 个分类器，每个分类器的对应识别输出为 $R_m(m=1,2,\cdots,M)$。未知模式 x 能且只能被识别为 N 类模式中的某一类，N

类模式出现的先验概率 $P(X_n)(n=1,2,\cdots,N)$ 设为相等。根据贝叶斯理论未知模式将被识别为后验概率最大的第 n 类模式 X_n，即：

$$n=\arg(\max_{i=1,2,\cdots,N}P(X_i\mid R_1,R_2,\cdots,R_M)) \tag{9.1}$$

其中的后验概率为：

$$\begin{aligned}&P(X_i\mid R_1,R_2,\cdots,R_M)\\&=P(R_1,R_2,\cdots,R_M\mid X_i)P(X_i)/P(R_1,R_2,\cdots,R_M)\\&=P(R_1,R_2,\cdots,R_M\mid X_i)P(X_i)/\left[\sum_{j=1}^{N}P(R_1,R_2,\cdots,R_M\mid X_j)P(X_j)\right]\\&=P(R_1,R_2,\cdots,R_M\mid X_i)/\sum_{j=1}^{N}P(R_1,R_2,\cdots,R_M\mid X_j)\end{aligned} \tag{9.2}$$

假设分类器识别输出相互独立，上式可以写为：

$$\begin{aligned}P(X_i\mid R_1,R_2,\cdots,R_M)&=\prod_{j=1}^{M}P(R_j\mid X_i)/\sum_{j=1}^{N}\prod_{k=1}^{M}P(R_k\mid X_j)\\&=\prod_{j=1}^{M}P(X_i\mid R_j)/\sum_{j=1}^{N}\prod_{k=1}^{M}P(X_k\mid R_j)\end{aligned} \tag{9.3}$$

将式（9.3）代入式（9.1）得：

$$n=\arg_i(\max_{i=1,2,\cdots,N}\prod_{j=1}^{M}P(X_i\mid R_j)) \tag{9.4}$$

将后验概率 $P(X_i\mid R_j)$ 二值化，并注意到 $\prod_{j=1}^{M}P(X_i\mid R_j)\leqslant\max_{i=1,2,\cdots,N}P(X_i\mid R_j)$，则多分类器融合的投票方法为：

$$\text{vote}_{ij}=\begin{cases}1 & k=\arg_i(\max_{i=1,2,\cdots,N}\prod_{j=1}^{M}P(X_i\mid R_j))\\0 & \text{otherwise}\end{cases} \tag{9.5}$$

$$n=\arg_i(\max_{i=1,2,\cdots,N}\prod_{j=1}^{M}\text{vote}_{ij}) \tag{9.6}$$

实例 2：信息融合在人脸识别中的应用

1）基于特征融合的人脸识别

事实上，对同一模式所提取的不同特征向量总是能反映模式的不同特性，对它们的有效融合，既可保留参与融合的多特征的有用信息，又可在一定程度上消除由于主客观因素带来的冗余信息，显然对分类识别具有重要的意义。每一种特征融合方法实质上是实现各个提取到的特征向量的关联、融合。下面是一个基于特征融合人脸识别的实例。

传统的串行特征融合的缺点是急剧地增加了组合特征的维数，增大了计算量，针对这一缺点，很多学者提出并行特征融合技术，其一般框架为：设 $\boldsymbol{A},\boldsymbol{B}$ 为特征样本空间 Ω 上的两组特征，任意样本 $\xi\in\Omega$，相应的两个特征向量为 $\boldsymbol{\alpha}\in\boldsymbol{A}$ 和 $\boldsymbol{\beta}\in\boldsymbol{B}$。用负向量 $\boldsymbol{\gamma}=\boldsymbol{\alpha}+\mathrm{i}\boldsymbol{\beta}$（i 为虚数单位）来表示 ξ 的并行组合特征。如果两组特征 $\boldsymbol{\alpha}$ 和 $\boldsymbol{\beta}$ 的维数不等，则低维的特征向量用 0 补足。例如，$\boldsymbol{\alpha}=\left[a_1,a_2,a_3\right]^{\mathrm{T}}$，$\boldsymbol{\beta}=\left[b_1,b_2\right]^{\mathrm{T}}$，则组合特征为 $\boldsymbol{\gamma}=\left[a_1+\mathrm{i}b_1,a_2+\mathrm{i}b_2,a_3+\mathrm{i}0\right]^{\mathrm{T}}$。样本空间 Ω 上的组合特征空间定义为 $C=\left\{\boldsymbol{\alpha}+\mathrm{i}\boldsymbol{\beta}\mid\boldsymbol{\alpha}\in\boldsymbol{A},\boldsymbol{\beta}\in\boldsymbol{B}\right\}$，显然，该空间为 n 维复向量空间，其中 $n=\max\left\{\dim\boldsymbol{A},\dim\boldsymbol{B}\right\}$，同一样本的两特征 $\boldsymbol{\alpha}$，$\boldsymbol{\beta}$ 组合可以有两种不同的方式：$\boldsymbol{\alpha}+\mathrm{i}\boldsymbol{\beta}$ 或者 $\boldsymbol{\beta}+\mathrm{i}\boldsymbol{\alpha}$，这就涉及酉空间内的并行特征组合的对称性问题[19]。

此处列举一种用于人脸识别的非线性鉴别特征融合方法。首先利用小波变换和奇异值分解获取同一样本空间的两类特征，然后利用复向量将这两类特征组合在一起，构成一个复特征向量空间，最后在该空间中利用改进的核 Fisher 鉴别分析进行最优非线性鉴别特征的抽取。

设 $\boldsymbol{A},\boldsymbol{B}$ 为经小波变换和奇异值分解后得到的两类低维特征向量，任意一个原始训量模式样本 X，它对应的两个特征向量分别为 $\boldsymbol{\alpha}\in\boldsymbol{A}$ 和 $\boldsymbol{\beta}\in\boldsymbol{B}$，用复向量 $\boldsymbol{\gamma}=\boldsymbol{\alpha}+\mathrm{i}\theta\boldsymbol{\beta}$ 来表示 X 的融合特征，其中 θ 为权重系数。注意，如果两组特征 $\boldsymbol{\alpha}$ 和 $\boldsymbol{\beta}$ 的维数不等，则低维的特征向量用 0 补足。

由于特征抽取方法与量纲选择的不同，导致了参与融合的同一模式样本的两类特征 $\boldsymbol{\alpha}$ 与 $\boldsymbol{\beta}$ 之间在数量关系上可能存在较大差别，如 $\boldsymbol{\alpha}=(20,10,15)$，$\boldsymbol{\beta}=(0.2,0.3,0.5)$。若直接以 $\boldsymbol{\gamma}=\boldsymbol{\alpha}+\mathrm{i}\boldsymbol{\beta}$ 的方式进行组合，两类特征融合后的比重明显失调。为了消除参与融合的两类特征在数值上的非均衡性造成的不利影响，有必要对 $\boldsymbol{\alpha}$ 与 $\boldsymbol{\beta}$ 分别进行一定的标准化处理，一种有效的方法是：

（1）令 $\boldsymbol{\alpha}'=\boldsymbol{\alpha}/\|\boldsymbol{\alpha}\|$，$\boldsymbol{\beta}'=\boldsymbol{\beta}/\|\boldsymbol{\beta}\|$，将 $\boldsymbol{\alpha}$ 与 $\boldsymbol{\beta}$ 化为单位向量；

（2）设 $\boldsymbol{\alpha}$ 与 $\boldsymbol{\beta}$ 的维数分别为 n 和 m，若 $n=m$，则取组合系数 $\theta=1$；否则，若 $n>m$，则取组合系数 $\theta=n^2/m^2$，融合形式为 $\boldsymbol{\gamma}=\boldsymbol{\alpha}+\mathrm{i}\theta\boldsymbol{\beta}$。

融合后的样本空间定义为 $C=\left\{\boldsymbol{\alpha}+\mathrm{i}\boldsymbol{\beta}\mid\boldsymbol{\alpha}\in\boldsymbol{A},\boldsymbol{\beta}\in\boldsymbol{B}\right\}$，明显地，该空间为 n 维复向量空间，其中 $n=\max\left\{\dim\boldsymbol{A},\dim\boldsymbol{B}\right\}$。之后选择相应的特征抽取方法与分类方法对融合后的特征进行特征提取及随后的分类识别。

2）基于决策融合的人脸识别

目前的研究已表明，红外人脸识别也是一种很好的生物鉴定技术。红外图像（也叫温谱图），它基于物体的温度分布，不受光照影响，甚至在黑暗中或有烟雾的情况下也有很好的性能，并能识别出伪装物、整形等。因此，即使在无法利用可见光进行识别的场合，它也能很好地工作。然而红外图像也有缺点，易受眼镜、周围环境温度的干扰。因此，对红外和可见光人脸进行融合识别，可以充分利用两类传感器的有用信息，从而提高系统的识别率。

这里列出一种应用 D-S 证据理论的决策融合识别方法，首先采用主成分分析（PCA）分别对两类图像提取主分量；然后计算测试样本与各类之间的欧氏距离，通过构造的函数实现欧氏距离到客观证据的转换；最后再用 D-S 证据理论对客观证据进行融合做出最优决策。假设在融合识别前，红外和可见光图像已经过严格配准。融合识别算法流程如下[20]。

Step 1：提取人脸特征。

采用 PCA 算法将测试样本 Γ 在特征空间进行投影，提取测试样本的低维主分量：

$$\boldsymbol{\Omega}^{\mathrm{T}} = \{\omega_1, \omega_2, \cdots, \omega_M\}$$

由于提取的主分量中每个特征元素具有不同的物理意义，它们的幅度可能差别较大，在相似性度量时会产生很大的偏差，所以必须进行特征归一化来消除这种偏差，使特征向量内部各分量在相似度量时具有相同的地位，即：

$$\boldsymbol{v} = \boldsymbol{\Omega} / \sqrt{\boldsymbol{\Omega}^{\mathrm{T}} \bullet \boldsymbol{\Omega}}$$

Step 2：获取子决策。

为了进行决策融合，需要得到各传感器提供的客观证据。因此，先计算测试样本到各类的欧氏（Euclid）距离作为它们之间的相似性度量：

$$D_i = \| \boldsymbol{v}^{\mathrm{T}} - \boldsymbol{v}_i^{\mathrm{T}} \|, \quad i = 1, 2, \cdots, N$$

其中，$\boldsymbol{v}^{\mathrm{T}}$ 为测试样本的主分量，$\boldsymbol{v}_i^{\mathrm{T}}$ 表示类 i 的主分量，可通过求该类训练样本的主分量平均值得到；N 为类别数。

然后，构造一个转换函数 $f(D_i)$ 实现从欧氏距离 D_i 到概率 $p(C_i \mid \Gamma)$ 的转换：

$$p(C_i \mid \Gamma) = f(D_i), \quad i = 1, 2, \cdots, N$$

C_i 表示第 i 类，D_i 为测试样本主分量到第 i 类样本主分量的欧氏距离，$p(C_i \mid \Gamma)$ 表示测试样本 Γ 属于第 i 类的概率，且 $0 \leqslant p(C_i \mid \Gamma) \leqslant 1$。

根据实验分析，转换函数 $f(D_i)$ 满足 0 均值的正态分布，即 $f(D_i) - N(0, \sigma^2)$，σ 可按实验数据求取。此方案中，选取 $\sigma_1 = 0.6$，$\sigma_2 = 0.7$，分别构造了红外和可见光传感器的转换函数 $f(D_i)$。

Step 3：决策融合。

将概率分布 $p(C_i \mid \Gamma)$ 作为决策级融合的客观证据。在运用 D-S 证据理论时，首先定义识别框架 Θ 为包含训练库中所有样本类别的集合，并设置红外和可见光传感器的置信度 $g_1 = 0.7$， $g_2 = 0.6$，分别来源于对单传感器的实验数据统计分析， $p(C_i \mid \Gamma)$ 为基本概率分配函数值，然后根据证据理论的组合规则对基本概率分配函数进行组合，得到组合后的基本概率赋值 $m(P_i)$。

用 D-S 证据理论组合证据后如何进行决策是与应用密切相关的问题。常用的决策方法有：基于信任函数的决策，基于基本概率赋值的决策和基于最小风险的决策等，可根据具体问题选取。在该方案中，我们综合考虑了这几种决策方法的性能后，最后采用基于基本概率赋值的决策规则进行决策。

设 $m(P_i)$ 为基于 D-S 证据理论组合规则得到的组合后的基本概率赋值， $\exists P_1, P_2 \subset \Theta$ 满足：

$$m(P_1) = \max\{m(P_i), P_i \subset \Theta\}$$

$$m(P_2) = \max\{m(P_i), P_i \subset \Theta, P_i \neq P_1\}$$

若满足：

$$\begin{cases} m(P_1) - m(P_2) > \varepsilon_1 \\ m(\Theta) < \varepsilon_2 \\ m(P_1) > m(\Theta) \end{cases}$$

则 P_1 即为判决结果，其中 ε_1， ε_2 为预先设定的阈值，根据经验分别选择 $\varepsilon_1 = 0.1$， $\varepsilon_2 = 0.3$。

9.4.3 语音处理与说话人识别中的应用

识别率和对环境的适应能力是语音识别系统的两个重要性能。近年来，人们提出各种各样的语音识别方法，常见的提高识别率的方法一般都着眼于改进声音模型来获得较高的识别率，这往往造成声音模型的复杂化及模型训练的困难。另外，常见的语音识别方法大多数都局限于安静环境、说话人对于麦克风的距离较近且位置相对固定等条件下的语音识别率提高的研究。这些方法在环境复杂、说话人和麦克风的位置较远、距离不固定的情况下往往效果很差。

借用信息融合这种模仿人类大脑处理信息的思想，很多学者提出了各种基于信息融合技术的语音处理与说话人识别方案[21~23]。

实例 1：基于信息融合的多话筒汉语语音音节识别方法[21]

该方法通过多个话筒分别采集声音数据，对每一个话筒分别建立声音模型，分别进行识别，然后用信息融合技术对各个模型的识别结果进行处理，以达到提高最终识别率和对环境适应能力的目的。和基于单一话筒的识别系统相比，该方法不仅具有在各个单独声音模型识别率不高的情况下，仍可以获得较高的音节识别率的优点，而且，由于采用多话筒技术，一方面可以较好地克服说话方向、轻重不同等所造成的识别率下降问题，另外还降低了对各个模块的识别率的要求，减轻了声音模型的训练困难。

1）多话筒语音识别的原理

多话筒语音识别的原理如图 9.5 所示。声音数据经由麦克风采集，被送到各自的特征提取器中提取特征，提取出来的特征被送到各自的声音模型进行识别，得出各个模型的初步识别结果 d_i，这些初步识别结果被作为候选送入融合中心进行数据融合，融合中心根据一定的融合算法对候选结果进行处理，得到最后的识别结果 t。

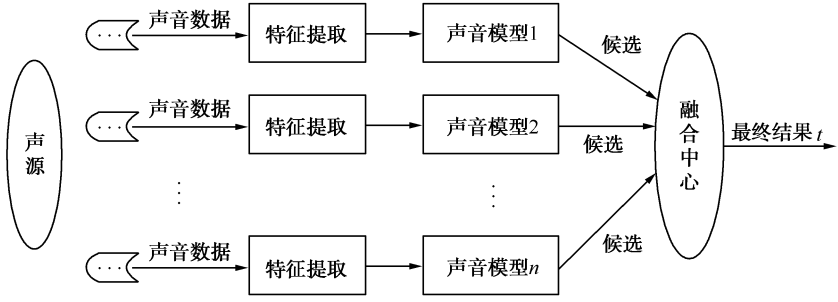


图 9.5　多话筒语音识别的原理

2）声音模型

声音模型采用一种改进的递归神经网络——时间标签递归神经网络（TTRNN）来对汉语音节进行分类。时间标签递归神经网络结构如图 9.6 所示，这是一个一阶时延的 TTRNN。其中，Time-Tag 单元为时间标签发生器，为每一帧输入 $u(t)$ 产生一个时间标签。语音的每一帧 $u(t)$ 及前一帧所产生的反馈输出 $x(t)$ 被输入 TTRNN，得出在时刻 t 输入 $u(t)$ 在反馈输入为 $x(t)$ 时属于某个分类的概率 $P_k(u(t))$，以及时延反馈输出 $x(t+1)$。则整个时序模式 u 属于某个分类的概率为：

$$P_k(u) = p_k(u(1)) \times p_k(u(2)) \times \cdots \times p_k(u(n)) = \prod_t p_k(u(t)) \tag{9.7}$$

图 9.6 中在输出节点上的圆圈表示计算式（9.7）的过程。

用 TTRNN 对汉语音节进行分类，就是要求一个汉语音节属于各个分类的概率，根据概

率的不同，可以确定该汉语音节属于哪一类。由式（9.7）知，若要求 $P_k(u)$，只需求出 $P_k(u(t))$ 即可，而这可以由 TTRNN 来得到。

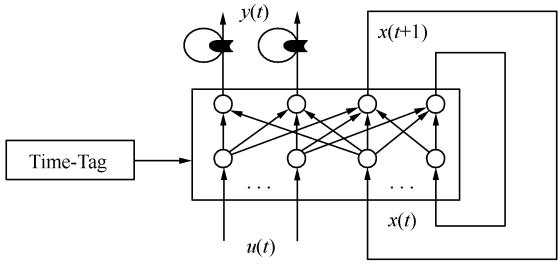


图 9.6　时间标签递归神经网络结构

3）融合算法

前端的声音模块对输入进行初步识别，得到初步的识别结果 $d_i\,(i=1,2,\cdots,N)$，组成候选集 D，被送到融合中心进行最后的判决，得到最终识别结果 t。我们用 $H_j\,(j=1,2,\cdots,m)$，表示 m 个类，其中 $H_j\,(j=1,2,\cdots,m-1)$ 表示有信号假设类，而第 m 个类 H_m 表示无信号假设类。

设各个声音模块是统计独立的，融合中心在候选集 D 的基础上根据一定的融合算法得到整个系统的最终识别结果，即：

$$t = f(d_1, d_2, \cdots, d_N) \tag{9.8}$$

设

$$L_j(D) = \log_2 \frac{P(H_j \mid D)}{P(H_m \mid D)} = \log_2 \frac{P(H_j \mid d_1, d_2, \cdots, d_N)}{P(H_m \mid d_1, d_2, \cdots, d_N)} \tag{9.9}$$

为 H_j 的概率似然比，其中 $j=1,2,\cdots,m-1$，根据最大似然比判决准则，融合中心的判决规则是：

$$t = \begin{cases} m & \text{if } L_j(D) < 0 \quad \forall j, j \neq m \\ \arg\max\limits_{j=1,\cdots,m-1}(L_j(D)) & \text{otherwise} \end{cases} \tag{9.10}$$

由式（9.10）可知，要想用该判决规则进行数据融合，只要求出 $L_j(D)$ 即可。下面讨论怎样求出 $L_j(D)$。设

$$\begin{aligned} S_1 &= \{i \mid d_i = j, \forall i = 1, \cdots, N\} \\ S_2 &= \{i \mid d_i = m, \forall i = 1, \cdots, N\} \\ S_3 &= \{i \mid d_i = l, \forall i = 1, \cdots, N, l \neq j \neq m\} \end{aligned} \tag{9.11}$$

则有：

$$
\begin{aligned}
P(H_j \mid D) &= \frac{P(H_j \mid D)}{P(D)} = \frac{P(H_j)}{P(D)} \bullet \prod_{i=1}^{N} P(d_i \mid H_j) \\
&= \frac{P(H_j)}{P(D)} \bullet \prod_{S_1}^{N} P(d_i = j \mid H_j) \bullet \prod_{S_2}^{N} P(d_i = m \mid H_j) \bullet \prod_{S_3}^{N} P(d_i = l \mid H_j) \\
&= \frac{P(H_j)}{P(D)} \bullet \prod_{S_1} P_{D_{jj}}^{i} \bullet \prod_{S_2} P_{M_{jm}}^{i} \bullet \prod_{S_3} P_{E_{jl}}^{i}
\end{aligned}
\tag{9.12}
$$

其中，$P_{D_{jj}}^{i} = P(d_i = j \mid H_j)$ 为前端声音模块 i 正确做出 j 类判决的概率；

$P_{M_{jm}}^{i} = P(d_i = m \mid H_j)$ 为前端声音模块 i 将 j 判决为无信号 m 类的概率；

$P_{E_{jl}}^{i} = P(d_i = l \mid H_j)$ 为前端声音模块 i 将 j 判决为 l 类的概率。

同理有：

$$
\begin{aligned}
P(H_m \mid D) &= \frac{P(H_m)}{P(D)} \bullet \prod_{S_1}^{N} P(d_i = j \mid H_m) \bullet \prod_{S_2}^{N} P(d_i = m \mid H_m) \bullet \prod_{S_3}^{N} P(d_i = l \mid H_m) \\
&= \frac{P(H_m)}{P(D)} \bullet \prod_{S_1} P_{F_{mj}}^{i} \bullet \prod_{S_2} P_{D_{mm}}^{i} \bullet \prod_{S_3} P_{E_{ml}}^{i}
\end{aligned}
\tag{9.13}
$$

其中，$P_{F_{mj}}^{i} = P(d_i = j \mid H_m)$ 为前端声音模块 i 将无信号 m 判决为 j 类的概率，$j \in S_1$；

$P_{D_{mm}}^{i} = P(d_i = m \mid H_m)$ 为前端声音模块 i 正确判决为无信号 m 的概率；

$P_{E_{ml}}^{i} = P(d_i = l \mid H_m)$ 为前端声音模块 i 将无信号 m 错判决为 l 类的概率，$l \in S_3$。

由式（9.9），式（9.12），式（9.13）有：

$$
L_j(D) = \log_2 \frac{P(H_j)}{P(H_m)} + \sum_{S_1} \log_2 \frac{P_{D_{jj}}^{i}}{P_{F_{mj}}^{i}} + \sum_{S_2} \log_2 \frac{P_{M_{jm}}^{i}}{P_{D_{mm}}^{i}} + \sum_{S_3} \log_2 \frac{P_{E_{jl}}^{i}}{P_{E_{ml}}^{i}} \tag{9.14}
$$

其中，$P_{D_{jj}}^{i}$，$P_{M_{jm}}^{i}$，$P_{E_{jl}}^{i}$，$P_{F_{mj}}^{i}$，$P_{D_{mm}}^{i}$，$P_{E_{ml}}^{i}$ 可以通过统计得到。

实例 2：马尔可夫模型（CHMM）在多种参数信息融合中的应用[22]

提高语音识别系统的鲁棒性是语音识别技术走向实用的关键问题，因而如何提高系统的鲁棒性正成为语音识别的研究热点。语音识别系统的鲁棒性主要包括对环境的鲁棒性和对说话人的鲁棒性两个方面。目前，鲁棒性语音识别通常是将多种特征参数结合起来使用，例如，将 MFCC 特征参数和它的差分型特征参数（ΔMFCC）构成一个大的特征矢量。模型一般都使用各种类型的 HMM 模型，因为 HMM 模型能较好地刻画语音信号中的时序信息。但是 HMM 也有它的不足之处，例如，它认为各帧矢量之间是独立同分布的，这就与实际情况不符。另外，在描述 HMM 模型的参数 $\boldsymbol{\lambda} = (\pi, \boldsymbol{A}, \boldsymbol{B})$ 中，$\boldsymbol{A}$ 矩阵是各状态之间的转移概率矩阵，它在

HMM 模型中被看成静态的，但我们认为随着模型在一个状态上停留时间的增加，模型应该更倾向于向后面的状态跳转而不是继续停留在这个状态上。因此，$\boldsymbol{A}$ 矩阵应该随着计算帧数的增加而不断被修正，即它应该是动态的。下面给出一个利用改进后的 CHMM 模型对不同的特征参数携带的信息进行信息融合的实例。

1）MFCC 和ΔMFCC 的抗噪性比较

MFCC 参数是目前应用最为广泛的特征参数。其特点是，在高信噪比的条件下，MFCC 特征参数具有很好的识别率，但在信噪比低的时候，识别性能很差。而ΔMFCC 参数则在低信噪比时，能有较好的识别率，但在高信噪比时识别率不如 MFCC。目前鲁棒性说话人识别中，一般是将 MFCC 和ΔMFCC 两种参数构成一个大的特征参数。但是在同一文本条件下，将这两种参数赋予不同的比例后，其性能是不同的。而在不同文本的条件下，系统达到最佳性能的比例也是不同的。

2）利用改进的 CHMM 进行信息融合

为了充分发挥 MFCC 和ΔMFCC 的特点，一种可行的方案是利用改进的马尔可夫模型来综合这两种参数的信息。其主要思想是：由于 MFCC 在低噪声环境下性能更好，因此让它在低噪声的环境下，发挥的作用大一些，而在强噪声环境下，MFCC 受的干扰大，让它作用的比重降低。对于ΔMFCC 则相反。

我们知道，在以 MFCC 为特征参数的 CHMM 模型中，每个状态都用一个混合的高斯密度函数来描述该状态输出的观察矢量的分布。由于ΔMFCC 是通过 MFCC 进行差分得到的，可以认为ΔMFCC 特征参数对应着状态之间的转移。因此，对 CHMM 模型进行了修改，将状态转移弧也看成一种随机过程，用相应的概率密度函数来和ΔMFCC 特征参数联系。也就是说，用 Δ MFCC 来给出发生某个状态转移的置信度。这样当 MFCC 参数受到噪声干扰而偏离无噪声情况下训练得到的均值较大时，由于超出了状态概率密度函数的有效区域（球域），状态的概率密度函数只给出一个默认值，这时抗噪性好的ΔMFCC 将起主导作用，由它来确定当前的状态转移路径。这样，整个模型就能在强噪声环境下获得接近或超过ΔMFCC 在相同环境下的识别性能，而在低噪环境下则由这两种参数共同确定模型的状态转移路径。这样在高信噪比时，MFCC 参数由于能和状态概率密度函数较好地吻合而起主导作用。

改进的 CHMM 模型如图 9.7 所示，每个圆圈代表 CHMM 中的一个状态，每个带箭头的线段表示状态的转移。每个状态的观察矢量为 MFCC 参数，每条转移弧的观察矢量为ΔMFCC 参数。

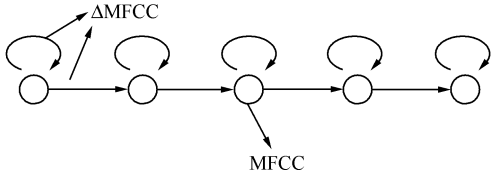


图 9.7　改进的 CHMM 模型

9.4.4　多生物特征认证中的应用

1．多生物特征认证举例

生物认证技术是指计算机利用人体所固有的生理特征或行为特征来进行身份识别的过程。与传统的认证方法相比，生物认证技术的最大特点就是对用户自身的特征进行认证，具有防伪性好、便于携带、不易丢失和遗忘的优点。但是，采用单生物特征进行认证的系统，普遍存在着可靠性和安全性等问题，这主要是由生物特征自身的稳定性和个体的特异性造成的。目前普遍采用两种方法解决这一问题，第一种方法是将生物认证和传统认证方式进行整合，但这种方法同时引入了传统认证的许多不利因素；第二种方法是采用多生物特征认证，对多个通道的生物特征在不同层次上进行信息融合。

在单生物特征认证的基础上发展多生物特征认证系统的时候，主要考虑以下几点：

（1）选择哪些通道作为整合的对象；

（2）选择的通道数目；

（3）整合多个生物特征时所采用的具体的整合方法；

（4）验证多生物认证系统所采用的生物特征数据库；

（5）多生物认证系统应用于具体场合的考虑。

接下来将介绍一种整合人脸图像和人的语音的多生物特征认证系统。就整合方法而言，一般的参考文献普遍采用了分数层和决策层的融合。适用于融合模块的算法很多，常用的有择多判决、贝叶斯估计、D-S 证据理论、模糊推理、支持向量机及人工神经网络等。在这里运用特征层的融合方法，且融合算法采用人工神经网络。

实例：基于神经网络的多特征生物认证系统

1）系统结构

该系统建立在多传感器信息融合的基础上，提取能良好表征人类个性特征的语音信号与人脸图像信息，运用人工神经网络的模式识别方法，对多源信息进行融合识别，以进行个体

身份验证。基于神经网络的多生物特征认证系统的框架如图 9.8 所示。

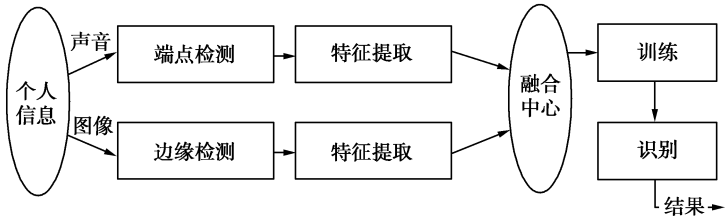


图 9.8 基于神经网络的多生物特征认证系统的框架

2）语音特征模型

在说话人识别问题中，关键问题是用语音信号的哪些特征来表征说话人，也就是特征提取问题。进行语音信号处理时，将说话人的声音用话筒或其他设备转化成电信号，再通过 A/D 转换使之成为离散的数字信号由计算机处理。

通过端点检测确定语音的起止点，把语音同背景噪声区分开来。语音信号是音源激励分量与声道冲激响应、辐射模型三者卷积的产物，因此通过语音信号的倒谱分析可以有效地分离激励与声道成分。所以，在众多的特征参数中，选择能较好反映说话人特征的 LPC 倒谱系数比较合适。

该系统采用 24 阶线性预测倒谱系数（LPC 系数）。求解语音信号的倒谱系数主要有两种方法。

（1）先对语音信号进行短时傅里叶变换，取其模的对数值，再进行反变换，得到倒谱系数。其中声道信息可通过低通滤波获取。

（2）依据 AR 模型对 LPC 参数进行递推，形成 LPC 倒谱，它的递推式如下：

$$\begin{cases} c(1)=a_1 \\ \quad \vdots \quad \vdots \\ c(n)=\sum_{k=1}^{n-1}(1-k/n)a_k \bullet c(n-k)+a_n \qquad (1<n\leqslant p) \end{cases} \tag{9.15}$$

式中，$a_1,a_2,\cdots,a_p$ 为 p 阶 LPC 特征向量，$c(n),n=1,2,\cdots,p$ 为倒谱的前 p 个值，当其取值 8～32 时可较好地表达声道特征。

LPC 倒谱的高阶分量具有较强的语音个性特征，经过 K-L 变换和最大可分变换后，各类特征参数在空间分布的散度进一步增大，这有助于压缩特征参数的个数，提高系统的性能。这里采用的是 K-L 变换，其实现步骤如下。

Step 1：求取特征向量协方差的估计。

$$\hat{S}_X = \frac{1}{N}\sum_{i}^{N_i}[\boldsymbol{x}-\hat{\boldsymbol{\mu}}_i][\boldsymbol{x}-\hat{\boldsymbol{\mu}}_i]^{\mathrm{T}} \tag{9.16}$$

Step 2：求其特征根和特征向量。

$$\hat{S}_X\boldsymbol{\phi}_i = \lambda_i\boldsymbol{\phi}_i \tag{9.17}$$

Step 3：由特征向量构成变换矩阵。

$$\boldsymbol{\phi} = [\boldsymbol{\phi}_1, \boldsymbol{\phi}_2, \cdots, \boldsymbol{\phi}_M] \tag{9.18}$$

3）人脸特征模型

在进行人脸图像分析前须做预处理，包括几何归一化和灰度归一化。几何归一化是指根据人脸定位结果将图像中的人脸变换到图像中同一位置和同样大小。灰度归一化是指解决图像中光照不均匀问题，经过归一化处理可改善图像质量，提高识别率。经校准不仅在一定程度上获得了人脸表示的几何不变性，而且还基本消除了头发和背景的干扰。在特征提取中，采取 PCA（Principle Component Analysis）方法，PCA 是统计学中分析数据的一种有效方法，其目的是在数据空间中寻找一组向量以尽可能地解释数据的方差，将数据从原来的 R 维空间降维投影到 M 维空间（$R \gg M$），降维后保存了数据的主要信息，使数据更易于处理。

将第 k 幅人脸图像输入看做一个一维向量，记做 $\overline{\boldsymbol{x}}_k$，记向量的协方差矩阵为：

$$\boldsymbol{W} = \frac{1}{N}\sum_{k=1}^{N}\{\boldsymbol{x}_k - \overline{\boldsymbol{x}}_k\}\{\boldsymbol{x}_k - \overline{\boldsymbol{x}}_k\}^{\mathrm{T}} \tag{9.19}$$

其中，$\overline{\boldsymbol{x}}_k = \frac{1}{N}\sum_{k=1}^{N}\boldsymbol{x}_k$，$N$ 为人脸图像总数。$\boldsymbol{W}$ 为对称矩阵，可对其进行对角化。

$$\boldsymbol{W} = \sum_{r}^{R}\lambda_r\overline{\boldsymbol{u}}_r\overline{\boldsymbol{u}}_r^{\mathrm{T}} = \boldsymbol{U}\boldsymbol{A}\boldsymbol{U}^{\mathrm{T}} \tag{9.20}$$

其中，λ_r 为 $\boldsymbol{W}$ 的特征值，$\overline{\boldsymbol{u}}_r$ 为相应的特征向量，$\{\overline{\boldsymbol{u}}_1, \overline{\boldsymbol{u}}_2, \cdots, \overline{\boldsymbol{u}}_R\}$ 为标准正交系，R 为 $\boldsymbol{W}$ 的秩，$\boldsymbol{A}$ 为对角阵，对角线上的元素为 $\boldsymbol{W}$ 的各特征值，将 $\overline{\boldsymbol{x}}_k$ 在 $\overline{\boldsymbol{u}}_r$ 上的投影记为 $\boldsymbol{P}_k^r$，则：

$$\boldsymbol{P}_k^r = \overline{\boldsymbol{u}}_r^{\mathrm{T}}\overline{\boldsymbol{x}}_k \tag{9.21}$$

令

$$\overline{\boldsymbol{P}}_k = (P^1, P^2, \cdots, P^R)^{\mathrm{T}} = \boldsymbol{u}^{\mathrm{T}}\overline{\boldsymbol{x}}_k \tag{9.22}$$

由 $\overline{\boldsymbol{P}}_k$ 的协方差矩阵可以得到 $\overline{\boldsymbol{x}}_k$ 在 $\overline{\boldsymbol{u}}_r$ 的投影的方差就是 $\overline{\boldsymbol{u}}_r$ 对应的特征值 λ_r，且各投影之

间互不相关。由于 $\sum_{i=1}^{R} W_{ii} = \sum_{i=1}^{R} \lambda_i$，定义方差贡献率：

$$\psi(M) = \frac{\sum_{i=1}^{M} \lambda_i}{\sum_{i=1}^{R} W_{ii}} \tag{9.23}$$

采用如下步骤进行特征抽取：①根据各幅人脸图像 $\bar{\boldsymbol{x}}_k$ 求出 $\boldsymbol{W}$；②求 $\boldsymbol{W}$ 的前 M 个最大特征值对应的特征向量，使 $\psi(M) > 0.8\ (R \gg M)$；③将各 $\bar{\boldsymbol{x}}_k$ 在 M 个特征向量张成的空间投影，得到 M 个投影值，以此 M 个投影值构成的向量 $\bar{\boldsymbol{x}}_k$ 作为原来图像的特征，即完成了高维（R 维）向低维（M 维）的转换。

4）基于神经网络的信息融合

与其他方法相比，神经网络模式识别方法的一个重要特点就是它能够较有效地处理很多非线性问题。

信息融合是将各种途径、时间和空间上获得的信息作为一个整体进行综合分析处理，为进一步决策及控制奠定了基础。在许多信息融合的应用场合，实时处理能力要求较高，数据量大，且常常以很高的速度到达检测设备，神经网络在很多情况下能满足这些要求。神经网络具有大规模的并行处理能力并能通过硬件加以实现，因此能对数据进行快速处理。在特征层融合的身份识别技术中，要求对不同传感器中提取的特征向量进行关联，由于传感器类型往往差别较大，对不同类型的数据进行非线性关联形成一个融合向量比较困难，而神经网络却具有这一特殊功能。神经网络能够实现一种特殊的非线性变换，即把输入空间变换到隐含层输出所形成的空间，使得在这个空间中其后的分类问题变得比较容易。这种变换是把一种特殊的特征提取准则最大化来实现的，可以看做是一种特殊的特征提取器。因此，神经网络在多传感器信息融合领域具有广阔的应用前景。

该实例选用 RBF 神经网络模型对数据进行融合处理。网络中的输入节点、隐含层节点和输出节点数分别为 N、L、M。其中隐含层单元的作用相当于对输入模式进行一次变换，将低维的模式输入数据变换到高维空间内，以利于输出层进行分类识别。隐单元的变换作用实际上可以看做是对输入数据进行特征提取。

RBF 隐单元使用的是非线性传输函数。这里，假设 RBF 隐单元的变换函数为常用的高斯函数，则其第 i 个单元对应的输出为：

$$z_i(t) = K(\| \boldsymbol{x}(t) - \boldsymbol{s}_i \|) = \exp\left[-\sum_{j=1}^{N} (x_i(t) - s_{ii})^2 \Big/ 2\alpha_i^2 \right] \tag{9.24}$$

式中，$z_i(t)$——第 i 个隐单元的输出（即径向基函数）；

$\boldsymbol{x}(t)$——第 i 个输入模式向量；

$\boldsymbol{s}_i$——隐含层中第 i 个单元的变换中心向量；

α_i——对应第 i 个中心向量的控制参数。

由于 RBF 网络中隐含层单元使用了非线性传输函数，这就使它在隐单元中心向量确定的情况下，网络只需要对隐含层至输出层的单层权值进行学习修正，所以它具有更快的收敛速度，是一种较有效的前馈网络。

关于多生物认证系统效率的验证所基于的数据库也是值得关注的一个问题。一般的多生物特征认证系统效率的得出都是基于自己本身设立的数据库的，所以在这里凭借最后的效率结果来比较若干不同方法的优劣性是毫无意义的。一种可以借鉴的方法是：采用自己设立的数据库，然后在这个数据库的平台上对各种不同的方法进行试验，最终得出试验结果。

2．未来多生物认证的研究方向

多生物认证最根本目的是为了提高生物认证系统的识别性能，进而提高系统的可靠性和安全性。目前的研究主要分为两大方向：其一是提高数据的质量，包括传感器层的原始数据和特征层的特征数据等，尤其是特征层融合的潜力有待进一步挖掘；其二是提高分类器或通道间信息融合的效率，在这一点上，匹配层融合显示了较大的优越性和乐观的发展前景，特征层融合有待进一步改进。

9.5　小结

信息融合技术是研究如何加工、协同利用多源信息，并使不同形式的信息相互补充，以获得对同一事物更客观、更本质的认识的信息综合处理技术，广泛应用于包括军事、生物身份认证、遥感图像处理、智能交通等多个领域。

信息融合技术的理论实现方法很多，但目前尚未形成具有普遍指导意义下的较为严格的原理和方法，多数都是针对某一种应用背景而产生的一种融合实现算法。多源信息融合技术还是一门不成熟的技术，对信息融合过程本身的功能与形式也还没有一个统一的定义，也还不能对一般信息融合建立通用的数学模型。

目前的信息融合实用系统大多以专家系统设计方法为实现基础，而且是以一种简单的方式合成信息，还没有充分、有效地利用多传感器所提供的冗余信息，许多工作仍处于探索或仿真性阶段。此外，在信息融合系统设计方面也还面临许多实际问题，如传感器测量误差模型的建立、复杂动态环境下系统的实时响应、大知识库的建立及其管理等。

参 考 文 献

[1] 李玉榕．信息融合与智能处理的研究．浙江大学博士学位论文，2001.
[2] 管天云．多传感器信息融合研究．浙江大学博士学位论文，1998.
[3] 王润生．信息融合．北京：科学出版社，2007.
[4] 程利民，孔力，李新德．信息融合方法及应用研究．传感器与微系统，2007,26(3)：4-9.
[5] 易正俊．多元信息智能融合算法．重庆大学博士学位论文，2002.
[6] Mark Bedworth and Jane O’Brien Jemity．The Omnibus Model: A New Model of Data Fusion. Proc 1999 International Conf. on Information Fusion, Sunnyvale Hilton Inn, Sunnyvale，Califomia, USAParis, France, July 1999.
[7] 潘巍，王阳生，杨宏戟．多模态信息融合的一般功能模型设计——于融合功能与信息层次．计算机工程与应用，2006,29：27-30.
[8] 仲崇权，张立勇，杨素英，赵文豪．多传感器分组加权融合算法研究．大连理工大学学报，2002,42(2)：179-182.
[9] Simon Maskell. A Bayesian approach to fusing uncertain, imprecise and conflicting information Information Fusion, 2008, 9(2):259-277.
[10] Ravi Vadapalli，PPing Luo，et al. Demonstration of grid-enabled ensemble Kalman Filter data assimilation methodology for reservoir characterization. Proceedings of the 15th ACM Mardi Gras conference, 2008:1-6.
[11] X.L. Zhao，J.Z. Zhou, et al. Application of Entropy-Based Markov Chains Data Fusion Technique in Fault Diagnosis. Proceedings of the 2008 International Conference on Computer Science and Software Engineering, 2008:569-572.
[12] E.Gregoire, S.Konieczny. Logic-based approaches to information fusion. Information Fusion, 2006, 7(1):4-18.
[13] Maria Nilsson.Characterising user interaction to inform information-fusion-driven decision support. Proceedings of the 15th European conference on Cognitive ergonomics, 2008:1-4.
[14] E. F. Nakamura, P. A. F. Loureiro, et al. Information fusion for wireless sensor networks: Methods, models, and classifications. ACM Computing Surveys, 2007, 39(3):1-55.
[15] P.Doherty, B.D.Keplicz, A.Szaas. Dynamics of Approximate Information Fusion. Lecture Notes in Computer Science, 2007:668-677.

[16] 孟章荣．军事应用中的多源信息融合技术．现代防御技术，2001, 29(2)：27-30.
[17] 方昱春，王蕴红，谭铁牛．融合人脸轮廓和区域信息改进人脸检测．计算机学报，2004,27(4)：482-491.
[18] 皇甫征声．基于信息融合的人脸自动检测识别方法研究及系统实现．重庆大学硕士学位论文，2003.
[19] Yang J.,Yang J.Y., Zhang D., Lu J.F.. Feature fusion: Parallel strategy vs. serial strategy. Pattern Recogniton,2003,36(6):1369-1381.
[20] 邱亚丹，敬忠良，陈雪荣，肖刚．基于决策级的多源人脸融合识别．计算机工程与应用，2006,27：219-221.
[21] 赵以宝，王祁，聂伟，孙圣和．一种基于数据融合的多话筒语音识别方法．计算机研究与发展，1999,36(9)：1148-1152.
[22] 刘鸣，戴蓓倩，李辉，陆伟，李霄寒．鲁棒性话者辨识中的一种改进的马尔可夫模型．电子学报，2002,30(1)：5-7.
[23] 鲍焕军，郑方．GMM-UBM 和 SVM 说话人辨认系统及融合的分析．清华大学学报（自然科学版），2008,48(S1)：693-698.

Chapter 10

第10章

人脸识别技术

人脸识别技术是对个人身份进行有效识别和鉴定的一种最自然、最直接的手段，在当今使用的各种利用人体生物特征进行身份识别和鉴定的方法中，人脸识别以其直接、友好、方便的特点得到了越来越多的重视。同时，由于利用人脸来进行识别可以将其他方法无法获得的人物表情和心理特征考虑在内，也使人脸识别具有了其他识别方法无法比拟的有效性、适应性和灵活性。

人脸识别被重视的另一个重要原因是其在经济、安全、社会保障、犯罪、军事等领域有着巨大的潜在的应用价值，尤其在需要对用户身份进行验证或识别的场合，如银行、海关和重要安全部门的身份验证，驾照、护照、身份证等证件的核对，自动门禁、安全监控、罪犯搜捕等领域，人脸识别技术都具有广泛的应用价值。以身份验证为例，传统的 PIN 码加个人密码的安全机制存在诸多弊端，如密码难记忆且易遗忘、可能被黑客攻破、密码可能被盗窃和破译等，尤其是为了便于记忆，人们通常以自己的生日和姓名等为密码，密码的安全性受到严重威胁。另外，在敲击密码的过程中，别有用心的人很容易窃取密码，如采用摄像机可以录下用户所输入的密码。由于上述原因，人们期待着能有一种低成本、安全和方便的身份识别方式，而人脸识别技术因其无需用户过多参与、非接触式的数据采集方式、对用户无任何损害和便于隐藏等优点而普遍为人们所看好，因此人脸识别技术被许多研究者称为 21 世纪最有前途的身份验证方法之一。

10.1　人脸识别概述

人脸识别技术问题一般可描述为：给定一个静止或动态人脸图像，利用某种方法对其进行处理，并和已存储的人脸数据库中图像进行匹配，从而确定给定图像中的人是不是指定的数据库里面的那个人（人脸确认 Face Authentication），或者是判断给定图像是数据库里面的哪个人（人脸辨认或人脸识别 Face Recognition）。人脸识别系统框图如图 10.1 所示。

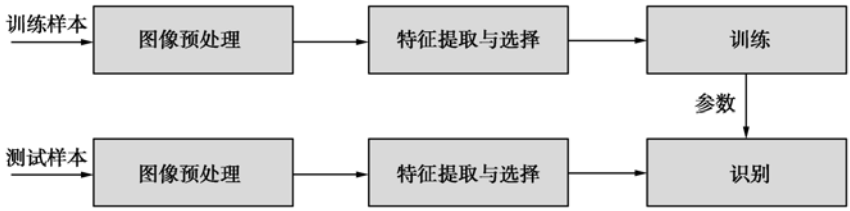


图 10.1　人脸识别系统框图

图 10.1 给出了人脸识别系统框图。人脸识别系统主要由 4 个功能模块组成，各模块所发挥的作用如下。

1）预处理模块

通过对样本图像或识别图像进行几何归一化、消除噪声和灰度归一化处理，消除或减小光照强度和方向、成像系统本身性能及外部环境等因素对待处理图像质量产生的干扰，使不同图像中人脸大小和亮度尽量统一，以便在相同的条件下完成训练和识别。

该模块的作用是为后续处理提供高质量的图像。

2）特征提取模块

采用某种策略，对经过预处理后的人脸图像进行分析，从中提取用于识别操作的特征，将原始的人脸空间中的数据映像到特征空间，其本质是通过从人脸图像空间到特征子空间的映像，对原始数据进行变换，以得到最能反映分类本质的特征，从而有效地实现分类识别，所提取特征的稳定性和有效性直接关系到识别效果的成败。

在提取特征的过程中，应根据不同的识别方法选取相应的特征形式。

（1）基于知识的提取方法：这一步主要是提取特征点，然后构造特征向量。

（2）模板匹配方法：用相关系数作为特征。

（3）子空间变换方法：将图像相关矩阵的特征向量在一定方向向量上投影，将得到的系数组成向量作为人脸特征，该方法有线性子空间和基于核函数的非线性子空间两种方法。

3）人脸图像训练模块

对已有人脸图像库中的人脸图像进行训练以便得到供识别模块完成判别的参数。该模块作为人脸识别研究的核心，与所采用的算法关系极大。

4）人脸识别模块

根据训练所得的参数完成人脸的最后判别，得出判别结果。

10.1.1 人脸识别研究现状

在自然界和人类社会中，经常会遇到这样一种现象：在完全相同的情况下，一个实验或观察（统称为实验）出现的结果可能是不同的。这种现象称为随机现象，其特点是：可重复观察，在观察之前知道所有可能的结果，但不知道到底哪一个结果会出现。这种现象是一种有客观条件决定的不确定现象，这是因为时间发生的条件不充分，使得条件与结果之间没有必然的因果关系，因而在事件的出现与否上表现出不确定性。

1．国外研究现状

国外对于人脸识别的研究起步较早，至今已经有多所大学或研究机构研制出了人脸识别原型系统，也开发出了一些商用的人脸识别系统，如德国的 Cognitec、美国的 Eyematic 和 Indentix 都投入了实际应用。此外，DCS AG 公司的 BioID 系统，通过数字摄像头和麦克风，采集一个人的面貌、声音及嘴唇运动三种生物特征，利用生物特征融合技术，在一秒钟内快速完成身份识别，可以满足更高的安全性要求。最主要的美国国防部发起的 FERET（Face Recognition Technology）和 FRVT（Face Recognition Vendor Test）人脸识别测试活动，也大大推动了人脸识别技术的应用和研究。

由美国国防部资助的 FERET 项目无疑是人脸识别研究领域中的一个至关重要的事件。FERET 项目的目标是要开发能够为安全、情报和执法部门使用的自动人脸识别技术。该项目包括三部分内容：资助若干项人脸识别研究，创建 FERET 人脸图像数据库，组织 FERET 人脸识别性能评测。该项目分别于 1994 年、1995 年和 1996 年组织了 3 次人脸识别评测，几种最知名的人脸识别算法都参加了测试，极大地促进了这些算法的改进和实用化。此外，FERET’96 人脸识别算法评估表明：主流的人脸识别技术对光照、姿态等非理想采集条件下的人脸识别的鲁棒性比较差。因此，光照、姿态问题逐渐成为热点研究方向。

与此同时，FERET 项目之后，涌现出了若干人脸识别商业系统，美国国防部有关部门进一步组织了针对人脸识别商业系统的评测——Face Recognition Vendor Test（FRVT），至今已经举办了三次：FRVT 2000、FRVT 2002 及 FRVT 2006 测试。FRVT 2002 测试表明：目前的人脸识别商业系统的性能仍然对于室内外光照变化、姿态、时间跨度等变化条件非常敏感，

大规模人脸库上的有效识别问题也很严重，这些问题仍然需要进一步的努力研究。FRVT 2006 共有来自 10 个国家的 22 个单位参加，国际上最著名的人脸识别公司，如德国的 Cognitec System GmbH、美国的 Identix Inc、美国的 Viisage，以及近来被 Google 收购的 Neven Vison 等公司都参加了该次测试。另外，国际上的一些知名公司，如韩国的三星公司、日本的东芝公司等也参加了该测试。在 22 个参加测试的单位中有 6 个是学术研究机构，包括美国的卡耐基 •梅隆大学、新泽西理工学院和休斯敦大学等。清华大学和北京大学也参加了该测试。FRVT 2006 的测试结果表明，在可控环境下，虹膜、静态人脸和三维人脸识别技术的性能是相当的。此外，FRVT 2006 还展现了不同光照条件下人脸识别性能的显著提高。特别值得一提的是，清华大学电子工程系作为国内唯一参加 FRVT 2006 评测的学术机构，其人脸自动识别系统的性能优于人类。

2．国内研究现状

国内自 20 世纪 90 年代以来，在国家自然科学基金和 863 计划等多方面的资助下，清华大学（电子系、自动化系和计算机系）、哈尔滨工业大学计算机系、中科院（计算所、自动化所）、南京理工大学、上海交通大学等很多单位展开了人脸识别技术研究，北京工业大学（信号与信息处理研究室）也在人脸检测方面取得了较好的研究成果，其和澳大利亚的新南威尔士大学联合提出的人脸检测技术已被国际 MPEG—7 接受作为标准。为了推动人脸识别研究的发展，国内已经举行过数届生物识别学术会议，中国科学院自动化研究所也发起成立了一个中国生物认证产业联盟。据国际生物识别产业协会估计，我国生物识别技术的软件和硬件市场，有望在 10 年内达到每年 20 亿美元的规模。但是，目前国内的研究水平仍低于国际水平，许多核心技术被国外大公司掌握。因此，研究开发具有自主知识产权的人脸识别技术是一个新的挑战。

10.1.2　人脸识别的最新进展

1．二维图像人脸识别

1）针对小样本问题的人脸识别研究

在过去的 20 多年里，人脸识别研究领域出现了许许多多令人鼓舞的成果。然而，仍然有一个问题困扰着研究人员，即高维小样本问题（Small Sample Size, SSS）。这主要是由于 2D 图像表征的人脸会由于光照、姿态、表情及年龄等因素的变化而呈现多变的特性。总的来说，高维小样本问题可以分为两类情形：第一类情形是各类训练样本数量小于特征子空间的维数；第二类情形是训练样本数大于子空间维数。第一类情形会造成类内及类间协方差矩阵不可逆。第二类情形会造成协方差矩阵的逆矩阵不稳定，这就导致不能直接使用二次判别分析法

（Quadratic Discriminant Analysis ，QDA）。为了解决各类协方差奇异问题，Friedman[1]提出了一种正则化判别分析方法（Regularized Discriminant Analysis，RDA），该方法是线性判别分析与二次判别分析的折中。RDA 通过对各类协方差与总体协方差之间的插值运算，解决各类协方差矩阵的奇异问题。然而，RDA 方法中的参数选取具有盲目性，未能实现优化选取[2]。针对 RDA 参数选择方面的缺陷，Ye[3]等人提出一种 RDA 模型参数的加速选择算法，他们将 RDA 计算过程分解为两步进行，实验结果验证了该方法的有效性。

解决小样本问题的一种有效方法是生成虚拟训练样本，近几年针对此类方法研究发展较快。Song[4]等人将眼睛作为人脸特征，随后采用基于遗传算法的 3D 合成方法产生了虚拟样本。Liu[5]采用加权的方法生成虚拟样本，将具有不同权重的虚拟样本看做训练样本。参考文献[2]提出了一种在特征子空间中通过对训练样本的扰动来生成虚拟样本的方法。

2）针对光照和姿态变化的人脸识别研究

FRVT 2002 的测试结果表明，光照的变化使人脸识别正确率从 90%下降到 50%。因此，光照问题成为人脸识别技术发展的瓶颈。截至目前，针对此类问题最常用的方法有光照锥方法（Illumination Cone）、球谱分析法（Spherical Harmonics）、明暗恢复形状法（Shape From Shading，SFS）及熵图像法（Quotient Image，QI）。

光照锥理论由光线方向的变化生成人脸图像的光照锥模型。理论上，该方法能获得完美的识别率，然而在光线任意变化的条件下，该方法需要至少 7 个不同的光照图像来建立光照锥模型，条件难以满足。Ramamooorthi 与 Basri[6]开发的球谱分析法给出了不同光照条件下的目标图像可以描述为低维子空间中的图像的原因。如果在每种姿态和不同光照下都有足够多的训练样本，球谱分析理论上能在某些人脸库上达到完美的识别效果。然而对于训练样本数目的要求限制了该方法的应用。明暗恢复形状法（SFS）能够从一幅或多幅二维输入图像汇总挖掘出三维人脸图像的深层次信息。由 Shashua 等人开发的熵图像法[7]是个能够抽取光照不变量特征的简单却又有效的方法。所谓熵图像是指一幅测试图像与三个非共面的光照图像之比，其中非共面光照图像依赖于漫反射系数（Albedo），该系数是光照不变量。熵图像法能够避免复杂的人脸建模并且达到较高的识别率，但它也存在一定的缺陷[8]：①该方法仅仅采用 3 个不同的人脸光照图来合成所有的光照条件下的结果，有时候不能满足极端的情形。②忽略了可能影响合成图像的面部阴影。③虽然该方法在理论上可以合成任意光照条件下的样本，然而缺乏理论证明。总体来讲，在熵图像方法中，不同人脸反射率之间的比率是个常数，该常数具有对变化光源的不敏感性，很适合用于人脸识别研究。

3）多模式（光谱）的人脸识别（红外图像、红外与可见光图像融合）研究

为了克服可见光人脸识别技术的不足（如光照变化引起的图像质量不高），目前有很多学者与组织对红外人脸识别技术展开了研究，在所有的红外谱方法中，长波红外（LWIR）图像显现出很多优良特性，从而补充了可见光人脸识别。LWIR 或热红外图像在光谱中占有 8～

12μm 的区段。出于这部分区段的图像能够表征目标的热模式并且对于光照和表情变化是不变的。如果能将 LWIR 的特性与可见光结合，将有助于提高人脸识别的效率。

目前已有很多文献比较了热红外图像与可见光图像在人脸识别中的性能。结果表明，在表情和光照变化的情况下，红外图像比可见光图像有更高的识别性能。而且，很多融合可见光和 LWIR 人脸图像的算法被提出：参考文献[9]提出了一种在像素层融合的方法；参考文献[10]则在特征层实现了可见光与 LWIR 图像的融合；参考文献[11]在分数匹配层及决策层实现了融合。基于多光谱的信息融合技术在人脸识别中较任何单一的方法而言（如可见光或红外光），均展现出了更高的性能。

2．三维图像人脸识别

就目前来说，人脸识别主要的进展还是局限于二维图像识别方面。因为人脸识别问题的复杂性，目前仍然很难建立一个具有鲁棒性的自动人脸识别系统。根据 FRVT 2006 提供的信息表明，在无约束的情况下，人脸识别的性能仍很难满足商业需求。而三维人脸识别在表情变化方面体现出来的鲁棒性使得该方法得到越来越多的关注。实际上，人脸图像不仅仅包括二维的纹理信息，更包括一些三维的形状信息。如果单单采用二维的方法进行人脸识别，势必丢失许多重要的信息。一个可取的方法是将人脸或头部描述成一个现实的三维模型，从而不仅仅包括了纹理信息与形状信息，甚至还能模拟人脸的表情所包含的结构信息。再者，已经出现了很多计算机图形学方面的技术，用于模拟表情变化，年龄及发型的不同，从而提供了识别变化个体的有效途径。

随着三维人脸图像获取设备的迅速发展，基于三维图像的人脸识别越来越引起人们的兴趣。在三维人脸识别技术中，图像的深度信息及表面特征被用来刻画样本，该思想是一种在三维空间中刻画人脸面部特征的非常有效的方法，对于提高当前人脸识别的性能有实际意义。此外，已经出现了能够同时捕获纹理和深度信息的三维图像传感器，从而导致多模态人脸识别技术的诞生。

一些克服三维人脸识别中表情变化的方法也随之出现。当表情变化时，人脸表面发生不同的变化：有些地方扭曲严重，而有些地方变化不大。Chang 等人[12, 13]将整个面部分解为若干子区域，鼻子周围的刚性区域用来匹配与组合，从而实现分类识别。然而，当表情变化时，他们的方法很难确定哪些是刚性区域，哪些不是。

建立可变形三维人脸模型是模拟人脸表情的另一个方法。Lu 等人[14]从人脸数据中的某种可控部分提取了可变形信息。从而产生人脸表情的可变形模板。识别的过程是比较测试样本与可变形模板的过程。Passalis 等人[15]及 Kakadiaris[16]等人分别采用一种带注释的人脸模型去拟合变化的人脸表面，然后通过拟合模型得到变形图像。一个多阶段配准算法及后期小波分析使得算法鲁棒性得到提升。在这些研究中，主要的问题是如何从视觉图像中建立一个参数

化的三维模型，这一点不容易实现。人脸表情变化使人脸表面以某种方式发生变形，这一点可以在人脸识别中加以利用。Bronstein 等人[17]基于几何不变量方式将人脸表面表征为等比例的变形，并且通过综合散碎的纹理及典型图像实现了多模态的人脸识别，而这些纹理与典型图像对表情变化而言是鲁棒的。Mpiperis 等人[18]提出了一种人脸表面的测地学两极表示法，这种表征方法试图在人脸表面等比例变形的情形下描述人脸的不变特征，匹配时需要定义在测地学平面上的表面属性。

3．视频图像人脸识别

视频序列的特点是：人脸图像分辨率较低，光照和姿态等变化较大。然而，相对于单个静止图像，视频序列能提供更多的信息，如同一个人拥有更多的图像；可以根据运动变化估计三维人脸结构；视频序列的时间连续性和识别对象身份的一致性为人脸识别提供信息；可以从低分辨率图像恢复出高分辨率图像；可以根据眼球的运动、姿态的变化等进行身份识别以防止基于静态图像的欺骗等。

迄今为止，提出了许多基于视频的人脸识别方法。通过对 MPEG 视频流的研究，李甚阳[19]提出了一种基于 MPEG 流的复杂背景无限制人脸跟踪系统，该系统首先利用直方图实现镜头分割，然后利用 MPEG 编码特性对在 I 帧中检测出来的人脸进行自动跟踪，实验表明该算法对遮挡和转动有一定鲁棒性。Biuk 等人[20]根据每人的序列在人脸本征空间中形成一个不同的特定轨迹，然后根据轨迹之间的梯度和距离的累积值的大小进行人脸识别。Li 等人[21]采用序列后验估计同时完成对象的跟踪和验证。对库中每个人的模板，首先将它匹配到输入视频的第一帧上，并用一个参数模型模拟相邻帧之间的仿射跟踪状态。应用 SIS（Sequential Importance Sampling）方法逼近并传播人脸的仿射跟踪状态，基于最大概率完成身份验证。Krüger 等人[22]提出了基于典型样本的概率方法识别视频序列中的人脸。该方法从每人的训练视频中自动地抽取一些典型样本，使其涵盖了视频序列的信息，对于后续的跟踪和识别处理，这些典型样本用做概率混合分布的中心，最后采用凝聚法（CONDENSATION ）求解概率模型并完成人脸识别。

10.2 人脸图像的预处理

人脸归一化作为预处理最重要的部分，其目标是要排除两类图像差异：由于输入设备成像机理不同带来的差异；由于拍摄形式和环境不同带来的差异。

10.2.1　尺寸归一化

经研究发现，图像预处理可显著提高特征脸人脸识别效果。人脸图像归一化作为图像预处理中最重要的内容被广泛地应用于各种应用系统。人脸图像归一化由尺寸归一化和光照归一化组成，其中光照归一化可以通过图像直方图规则化实现；而尺寸归一化目前大都通过基于两个瞳孔的仿射变化，使其相应姿态的人脸图像上两只眼睛瞳孔在相应固定位置来实现。这种方法的前提是人脸图像没有出现明显的变形，对各个方向的旋转缩放是同性的，这对于前视人脸图像是适合的，而对于多姿态的人脸图像来说，由于人脸姿态变化较大，其变形也较大，这种方法得到的归一化图像信息损失很大。针对多姿态人脸识别问题，有学者提出基于两个瞳孔和一个嘴唇为中心的三点仿射变换，使其相应姿态的人脸图像上眼睛和嘴巴各自的中心点在相应固定位置。

10.2.2　光照归一化

目前，光照变化是制约人脸识别系统性能的瓶颈。原因主要有两个方面：一方面是因为光照变化造成了人脸的类内差异甚至大于类间差异。Adini 等人研究表明，同一个人在不同的光照条件下得到的图像之间的差异，往往比不同人在同一成像条件下得到的图像之间的差异还要大；另一方面是光照变化本质上是一个无限维的，光照变化对人脸图像的影响，除了光源本身的因素外，还跟人脸表面的几何特征、反射率等诸多因素有关，其因素往往是非常复杂的。针对光照因素的研究，国内外学者提出了很多优秀算法，总体来讲有 3 种思路：①基于传统的图像预处理方法，如直方图均衡、Gamma 变换等，此类算法简单，但在性能上往往难以达到理想的效果；②提取对光照不敏感特征，如 Gabor 特征、边缘图 Edgemap 等，其中 Gabor 特征的确能在一定程度上抑止光照变化的影响，被广泛应用于人脸识别系统的特征提取模块，而边缘图会造成一定程度的信息损失，难以取得理想的效果；③基于光照的模型，典型的方法有光照锥（Illumination Cone）、球谐函数（Spherical Harmonic）、熵图像（Quotient Image）等模型，此类方法理论性较强，试图通过数学理论结合光度学理论，给光照变化建立统一的模型，其假设过多、过强，有较大的局限性，在实际场景中往往难以满足其条件，因而在实际中难以应用。

10.3 人脸识别的研究内容及方法

10.3.1 人脸检测

任何人脸识别系统首先都需要从输入信息中获取人脸的位置、大小。因此，人脸检测是人脸识别系统的第一个步骤，这一步骤所获得的精度与速度直接影响整个系统的性能。此外，人脸检测的应用也大大超越了人脸识别系统的范畴，在人脸表情识别系统、基于内容的检索、视频会议、三维人脸模型等方面也有重要的应用价值。总的来说，较常用的人脸检测技术可以分为以下几种。

1．几何特征

所谓人脸的几何特征指的是人脸面部器官在几何上体现的特征。基于几何特征的人脸检测可分为三种[23]：基于先验知识的方法、基于特征不变量的方法及基于模板匹配的方法。其中，基于先验知识的方法是将人脸面部器官之间的关系编码准则化的人脸检测方法。该方法是一种自上而下的方法，依据人脸面部器官的对称性、灰度差异等先验知识，制定出一系列的准则，当图像中的待测区域符合准则时，则被检测为人脸。基于特征不变量的方法着眼于检测面部的一些不变的特征，如眼睛、鼻子、嘴巴等，该方法是自下而上的，先利用各种手段寻找上述的不变特征，然后综合找到的这些不变特征来确定待检测区域是否是人脸。基于模板匹配的方法可以分为两类：预定模板方法和变形模板方法。预定模板方法首先制定出标准的模板，然后计算检测区域和模板的相关值，当相关值符合制定的准则时，就判断检测区域为人脸。变形模板首先制定出模板参数，然后根据检测区域的数据对参数进行修改直至收敛，以达到检测出人脸面部器官位置的目的。

2．肤色模型

根据有没有涉及成像过程，可以将肤色检测方法分成两种基本类型[24]：基于统计的方法和基于物理的方法。基于统计的肤色检测通过建立肤色统计模型进行肤色检测，主要包括两个步骤：颜色空间变换和肤色建模。基于物理的方法则在肤色检测中引入光照与皮肤间的相互作用，通过研究肤色反射模型和光谱特性进行肤色检测。

3．统计理论

基于统计理论的人脸检测是利用统计分析与机器学习的方法来寻找出人脸样本与非人脸样本各自的统计特征，再使用各自的特征构建分类器，最后采用特定的分类器完成人脸检测。

基于统计理论的人脸检测方法主要有[23]：子空间方法，神经网络方法，支持向量机方法，隐马尔可夫模型方法及 Boosting 方法。

10.3.2　特征提取

1．几何特征

基于知识的特征提取方法主要是根据人脸器官的形状描述，以及它们之间的距离特性来获得有助于人脸分类的特征数据，即几何特征，是最早、最传统的方法。几何特征是人脸的直观特征，基于几何特征的识别方法符合人类识别人脸的机理，易于理解；对每幅图像只需存储一个特征矢量，存储量小；另外，对光照变化不太敏感。早期的人脸识别研究主要是基于几何特征的，基于几何特征识别方法的主要缺点是：从图像中提取稳定的特征比较困难；对强烈的表情变化和姿态变化的鲁棒性较差；一般几何特征忽略了局部细微特征，造成部分信息丢失。

2．模板法

1）灰度模板

基于灰度模板匹配算法是图像匹配中常用的方法，但只适合于匹配简单的刚体或仿射变换的场景，并且对噪声、图像灰度变化较敏感，运算速度很慢。其优点是算法简单，能够利用相关值较好地表示两幅图像的相似程度。基于灰度模板匹配的方法常常利用人脸图像的灰度值进行相关运算，取相关系数大的目标图像为识别结果。在匹配以前，所有的图像都要进行相同的归一化处理，相关系数 C 的计算方法为：

$$C=\frac{<I_T,T>-<I_T><T>}{\sigma(I_T)\sigma(T)} \tag{10.1}$$

其中，I_T 是待识别图像，T 为模板图像，$<T>$ 指计算 T 中像素的平均值，$\sigma(T)$ 指的是求 T 的标准差，$<I_T><T>$ 指计算两图像中对应位置上像素值的乘积。

2）可变形模板

在人脸图像特征提取技术中，可变形模板得到了较为广泛的应用。其主要思想是根据人脸特征的先验形状信息，定义一个用若干参数描述的形状模型，这些参数反映了对应特征形状的可变部分，如位置、大小、角度等，它们最终通过模板与图像的边缘、峰、谷和灰度分布特性动态地交互适应得以修正。由于模板变形利用了特征区域的全局先验信息，因此可以较好地检测出相应的特征形状。

由于变形模板要采用优化算法在参数空间内进行能量函数极小化，因此算法有两个主要

缺点：一个是对参数初值的依赖程度高，容易陷入局部最小；另一个是计算时间较长。

3．线性的代数特征提取方法

1）PCA、LDA 子空间方法

人脸图像的维数通常是非常高的，而实际上人脸图像在这样高维空间中的分布很不紧凑，因而不利于分类，并且在计算上的复杂程度也非常大。为了得到人脸图像的较紧凑分布，Kirby 和 Turk 等人首次把主元分析的子空间思想引入到人脸识别中，并获得了成功。子空间分析的思想就是根据一定的性能目标来寻找一个线性或非线性的空间变换，把原始信号数据映射到一个低维空间中，使数据在该低维空间中的分布更加紧凑，该低维空间叫子空间。子空间分析除了有线性和非线性空间变换之分外，根据不同的性能目标要求，得到的子空间也是不一样的。主成分分析又叫 K-L 变换，目的是通过线性变换找一组最优的单位正交向量基（即主元），用它们的线性组合来重建原样本，并使重建后的样本和原样本的误差最小。在数学上，主成分分析就是通过解特征值问题来对角化协方差矩阵 $\boldsymbol{S}$ 的，

$$\boldsymbol{S}=\frac{1}{N}\sum_{i-1}^{C}(\boldsymbol{x}_i-\bar{\boldsymbol{x}})(\boldsymbol{x}_i-\bar{\boldsymbol{x}})^{\mathrm{T}} \tag{10.2}$$

$$\boldsymbol{\lambda w}=\boldsymbol{Sw} \tag{10.3}$$

其中，N 表示样本的总个数，$\bar{\boldsymbol{x}}$ 是所有样本的均值。把特征值按降序排列，$\lambda_i \geqslant \lambda_{i+1}$，选择对应前 m（通常 $m<N$）个非零特征值的特征向量作为主元。因此原空间的样本就可以用低维主元子空间上的投影系数 a_i 来描述。

$$\boldsymbol{y}=\sum_{i=1}^{m}a_i\boldsymbol{w}_i \tag{10.4}$$

主元分析在人脸识别上的应用最早是由 Kirby 等人提出来的，Turk 等人后来把它成功地发展为特征脸（Eigenfaces）方法，用于正面的人脸识别。特征脸的思想就是从训练图像中，通过主元分析得到一组特征脸图像（即对应的主元），那么任意给定的人脸图像都可以近似为这组特征脸图像的线性组合，用组合的系数作为人脸的特征向量。主元分析中主元选取的优先级通常是按对应的特征值大小来确定的，特征值越大，其优先级就越高。但是就人脸识别而言，应该选择多少个主元是最佳的，目前常用的标准有两种：① 当对应的特征值和最大的特征值相比小于一定值时就不要了；② 选择的特征值之和与总的特征值之和的比值要大于等于 0.9。

尽管主元分析在人脸识别中取得了不错的效果，但是由于它是以所有样本的最优重建为目的的，因此对于描述异类样本之间的差异而言，它不一定是最优的描述。从这个意义上来说，用它来描述人脸识别的特征是不充分的。

线性判决分析（LDA）不同于主元分析，从理论上来说，比较适合于模式识别。线性判

别分析的主要思想如下。

设有 C 个类别，每类 N 个样本，总样本数为 $M=CN$，$\boldsymbol{x}_m^i \in \mathbf{R}^d$ 为第 i 类的第 m 个样本。类间离散度、类内离散度和总散度矩阵分别定义为：

$$\boldsymbol{S}_b = \sum_{i-1}^{C} N(\boldsymbol{\mu}_i - \boldsymbol{\mu})(\boldsymbol{\mu}_i - \boldsymbol{\mu})^{\mathrm{T}} = \boldsymbol{\Phi}_b \boldsymbol{\Phi}_b^{\mathrm{T}} \tag{10.5}$$

$$\boldsymbol{S}_w = \sum_{i=1}^{C} \sum_{k=1}^{N} N(\boldsymbol{z}_k - \boldsymbol{\mu}_i)(\boldsymbol{z}_k - \boldsymbol{\mu}_i)^{\mathrm{T}} = \boldsymbol{\Phi}_w \boldsymbol{\Phi}_w^{\mathrm{T}} \tag{10.6}$$

$$\boldsymbol{S}_t = \boldsymbol{S}_b + \boldsymbol{S}_w \tag{10.7}$$

经典的线性判别分析中使用的是 Fisher 准则函数，所以线性判决分析又被称为 Fisher 线性判别分析（Fisher LDA 或 FLDA）。Fisher 准则函数定义为：

$$J(\boldsymbol{w}) = \arg\max_{\boldsymbol{w}} \frac{|\boldsymbol{w}^{\mathrm{T}} \boldsymbol{S}_b \boldsymbol{w}|}{|\boldsymbol{w}^{\mathrm{T}} \boldsymbol{S}_w \boldsymbol{w}|} \tag{10.8}$$

直接进行 LDA 面临两个问题：维数问题和小样本问题。Yu 和 Yang[25]在 2001 年提出了直接线性判别分析（Direct LDA 或 DLDA）法，其关键思想是要去掉 $\boldsymbol{S}_b$ 的零空间，保留 $\boldsymbol{S}_w$ 的零空间，即取 $\boldsymbol{S}_b$ 的非零空间和 $\boldsymbol{S}_w$ 的零空间的交集。因为 $\boldsymbol{S}_b$ 的零空间中不包含对分类有用的信息，而 $\boldsymbol{S}_w$ 的零空间包含了最重要的分类信息。

定理 1　对于任何一个 $n \times m$ 的矩阵，映射 $\boldsymbol{x} \to \boldsymbol{L}_x$ 是从 $\boldsymbol{L}^{\mathrm{T}}\boldsymbol{L}$ 的特征向量到 $\boldsymbol{L}\boldsymbol{L}^{\mathrm{T}}$ 的特征向量的一一映射，$\boldsymbol{x}$ 是 $\boldsymbol{L}^{\mathrm{T}}\boldsymbol{L}$ 的特征向量。

根据定理 1，就可以直接用 $\boldsymbol{\Phi}_b$ 和 $\boldsymbol{\Phi}_w$ 进行计算，大大方便了矩阵运算。

然而，从计算量的角度来看，DLDA 方法不适合处理高维的图像样本。这是因为算法的绝大部分都是在与图像展开向量相同维数的空间内进行的，一般原始图像空间的维数高达上万维，该算法所耗费的计算量是非常惊人的，所以当原始图像样本的维数较大时，需要先将图像映射到低维空间中，然后在低维空间中使用该算法。

2）奇异值分解

任何一个实对称方阵都可以通过正交变换化为对角矩阵。对于一般的矩阵也可以通过正交变换化为对角矩阵，这就是所谓的奇异值分解（Singular Value Decomposition）。

设 $\boldsymbol{A}_{m \times n}$ 是秩为 r 的实矩阵，则 $\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}$ 和 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$ 都是实对称的非负定方阵，因而它们的本征值都是非负的。假设 $\lambda_i^2 (i = 1, \cdots, r)$ 是矩阵 $\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}$ 的非零本征值，且按大小排列，并将 λ_i^2 对应的正交归一化本征向量记为 $\boldsymbol{u}_i$。由代数理论，λ_i^2 也是矩阵 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$ 的本征值，并且将对应的正交归一化本征向量记为 $\boldsymbol{v}_i$。于是有：

$$\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{u}_i = \lambda_i^2 \boldsymbol{u}_i, \quad \boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}\boldsymbol{v}_i = \lambda_i^2 \boldsymbol{v}_i \tag{10.9}$$

构造下述矩阵：

$$\boldsymbol{U}_{m\times n}=[\boldsymbol{u}_1,\boldsymbol{u}_2,\cdots,\boldsymbol{u}_r,\boldsymbol{u}_{r+1},\cdots,\boldsymbol{u}_m] \tag{10.10}$$

$$\boldsymbol{V}_{n\times m}=[\boldsymbol{v}_1,\boldsymbol{v}_2,\cdots,\boldsymbol{v}_r,\boldsymbol{v}_{r+1},\cdots,\boldsymbol{v}_n] \tag{10.11}$$

其中，$\boldsymbol{u}_i(i=r+1,\cdots,m)$ 与 $\boldsymbol{v}_i(i=r+1,\cdots,n)$ 是为了矩阵表达上的方便而引入的列向量，可以理解为 $\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}$ 与 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$ 分别对应于零本征值的正交归一化本征向量。显然，$\boldsymbol{U}$ 与 $\boldsymbol{V}$ 都是正交矩阵。由此可得：

$$\boldsymbol{A}=\boldsymbol{U}\sum\nolimits_{m\times n}\boldsymbol{V}^{\mathrm{T}} \tag{10.12}$$

其中，对角矩阵：

$$\sum\nolimits_{m\times n}=\mathrm{diag}[\lambda_1,\lambda_2,\cdots,\lambda_r,0,\cdots,0] \tag{10.13}$$

以上即为奇异值分解定理。

若矩阵 $\boldsymbol{A}_{m\times n}$ 代表一幅图像，可将 $\boldsymbol{A}$ 的所有奇异值组成 n 维向量：

$$\boldsymbol{X}_n=[\lambda_1,\lambda_2,\cdots,\lambda_r,0,\cdots,0]^{\mathrm{T}} \tag{10.14}$$

称为图像 A 的奇异值特征。

对于任意一个实矩阵 $\boldsymbol{A}$，它的奇异值分解是唯一的，所以当$\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_r$ 时，原图像 A 对应唯一的奇异值特征，于是可以用奇异值特征来描述和代表原图像的灰度值矩阵 $\boldsymbol{A}$。

3）基于二维图像矩阵的特征提取

一维方法在处理图像识别时存在固有的弊病。以人脸识别为例，人脸图像转换成向量后维数常常高达上万维，这会给随后的计算造成很大困难。虽然样本数较少时可以用奇异值分解（SVD）理论，将计算矩阵 $\boldsymbol{R}\boldsymbol{R}^{\mathrm{T}}$ 的本征值、本征向量问题转换为求解矩阵 $\boldsymbol{R}^{\mathrm{T}}\boldsymbol{R}$ 的问题，减少计算量，但实际中训练样本数可能同样很大，利用 SVD 理论也无法减少计算量。

对图像识别来说，近年来新出现的二维方法更直观，计算量更小，特征抽取的速度和效率更高。基于图像矩阵投影的二维方法的基本思想是利用数字图像矩阵直接构造图像散布矩阵，并在此基础上进行鉴别分析。

（1）2DPCA，采用 2DPCA 算法进行人脸图像特征提取，首先对训练样本图像进行标准化处理，随后求协方差矩阵，即：

$$\boldsymbol{G}=\frac{1}{m}\sum\nolimits_{i=1}^{M}(\boldsymbol{x}_i-\overline{\boldsymbol{x}})^{\mathrm{T}}(\boldsymbol{x}_i-\overline{\boldsymbol{x}}) \tag{10.15}$$

其中，$\boldsymbol{x}_i\in\mathbf{R}^{m\times n}$ 表示训练样本图像；$i=1,\cdots,M$，M 表示训练样本数；$\overline{\boldsymbol{x}}$ 表示所有训练样本的平均图像，即 $\overline{\boldsymbol{x}}=\frac{1}{M}\sum\nolimits_{i=1}^{M}\boldsymbol{x}_i$；训练样本的主元计算为 $\boldsymbol{U}^{\mathrm{T}}\boldsymbol{G}\boldsymbol{U}=\boldsymbol{\Lambda}$，其中，$\boldsymbol{G}\in\mathbf{R}^{m\times n}$，$\boldsymbol{\Lambda}$ 表

示特征值组成的对角阵，特征值表示为$\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_n$。

若特征值 $\lambda_i (i = 1,2,\cdots,n)$ 对应的特征向量表示为 $\boldsymbol{u}_i (i = 1,2,\cdots,n)$，则特征向量组成的特征矩阵为 $\boldsymbol{U}$，即 $\boldsymbol{U} = [\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_n]$。选择前 d 个较大特征值对应的特征向量构成特征矩阵 $\boldsymbol{U}_d = [\boldsymbol{u}_1, \boldsymbol{u}_2, \cdots, \boldsymbol{u}_d]$。训练样本 $\boldsymbol{x}_i \in \mathbf{R}^{m \times n}$ 向 $\boldsymbol{U}$ 投影，得到特征矩阵 $\boldsymbol{Y}_i$，即：

$$\boldsymbol{Y}_i = (\boldsymbol{x}_i - \overline{\boldsymbol{x}})\boldsymbol{U}_d \in \mathbf{R}^{m \times d} \tag{10.16}$$

任给一幅待测目标图像 $\boldsymbol{x} \in \mathbf{R}^{m \times n}$ 向 $\boldsymbol{U}$ 投影，得到其特征矩阵 $\boldsymbol{Y}$ 为：

$$\boldsymbol{Y} = (\boldsymbol{x} - \overline{\boldsymbol{x}})\boldsymbol{U}_d \in \mathbf{R}^{m \times d} \tag{10.17}$$

即完成了基于 2DPCA 的特征提取。

（2）2DLDA，设 $\boldsymbol{A}$ 表示一幅 $m \times n$ 的图像，$\boldsymbol{W}$ 为最优的 Fisher 投影矩阵。则 $\boldsymbol{A}$ 可以通过下式投影到 $\boldsymbol{W}$ 上：

$$\boldsymbol{y} = \boldsymbol{A}\boldsymbol{W} \tag{10.18}$$

从而，我们得到一个 m 维的映射向量 $\boldsymbol{y}$，称其为 $\boldsymbol{A}$ 的特征向量。

假设在训练集中有 c 个已知类别 T_i（i=1,2,⋯,c），N 为所有训练样本的数目。则第 i 类中的第 j 个训练样本可以表示为一个 $m \times n$ 的矩阵 $\boldsymbol{A}_j^i$ (j=1,2,⋯,N)，所有训练样本的均值为 $\overline{\boldsymbol{A}}$，$\overline{\boldsymbol{A}}^i (i = 1,\cdots,c)$ 表示第 i 类 T_i 的均值图像，N_i 为 T_i 中样本的数目。

2DLDA 尝试通过最大化如下的 Fisher 准则来寻找一个最优的鉴别矢量集，从而组成投影矩阵 $\boldsymbol{W}$：

$$\boldsymbol{J}(\boldsymbol{W}) = \frac{\boldsymbol{W}^{\mathrm{T}} \boldsymbol{S}_b \boldsymbol{W}}{\boldsymbol{W}^{\mathrm{T}} \boldsymbol{S}_w \boldsymbol{W}} \tag{10.19}$$

其中，

$$\boldsymbol{S}_b = \sum_{i=1}^{c} p_i (\overline{\boldsymbol{A}}^i - \overline{\boldsymbol{A}})^{\mathrm{T}} (\overline{\boldsymbol{A}}^i - \overline{\boldsymbol{A}}) \tag{10.20}$$

$$\boldsymbol{S}_w = \frac{1}{N} \sum_{i=1}^{c} \sum_{j=1}^{N_i} (\overline{\boldsymbol{A}}_j^i - \overline{\boldsymbol{A}}^i)^{\mathrm{T}} (\overline{\boldsymbol{A}}_j^i - \overline{\boldsymbol{A}}^i) \tag{10.21}$$

矩阵 $\boldsymbol{S}_b$ 与 $\boldsymbol{S}_w$ 分别为训练样本的类间散度矩阵和类内散度矩阵。p_i 为类 T_i 的先验概率。最优投影矩阵 $\boldsymbol{W}_{\mathrm{opt}}$ 的选择可以通过实现如下最优方程来得到：

$$\boldsymbol{W}_{\mathrm{opt}} = \arg\max_{\boldsymbol{W}} \boldsymbol{J}(\boldsymbol{W}) \tag{10.22}$$

最优问题式（10.22）可以通过对 $\boldsymbol{S}_w^{-1} \boldsymbol{S}_b$ 进行特征值分解，以及选取相应的 d 个最大特征值对应的特征向量来解决。

10.3.3 传统分类方法

1．贝叶斯决策[26]

人脸识别问题是一个多分类问题，每一个人脸的数据模型符合一个多维正态分布，如果对每一个类别分别建立一个多维正态模型，进行参数估计，则存在两个主要问题：一是类型数太大，问题复杂度高，二是每一个类的训练样本数太少，估计误差大。所以，在人脸识别问题中往往将多类分类问题转化为两类分类问题。将同一个人的不同的图像样本之间的差异称为内部差异，将不同的人的图像样本之间的差异称为外部差异，用 Ω_I，Ω_E 分别表示内部差异空间和外部差异空间。如果用向量 $\boldsymbol{I}_1$，$\boldsymbol{I}_2$ 表示两幅图像，$\boldsymbol{\Delta}=\boldsymbol{I}_1-\boldsymbol{I}_2$ 表示两幅图像的差值向量，$S(\boldsymbol{I}_1,\boldsymbol{I}_2)$ 表示图像的相似度，则 $S(\boldsymbol{I}_1,\boldsymbol{I}_2)=P(\boldsymbol{\Delta}\in\Omega_I)=P(\Omega_I\mid\boldsymbol{\Delta})$。$S(\boldsymbol{I}_1,\boldsymbol{I}_2)$ 是一个后验概率，则可以利用贝叶斯公式求出：

$$S(\boldsymbol{I}_1,\boldsymbol{I}_2)=\frac{P(\boldsymbol{\Delta}\mid\Omega_I)P(\Omega_I)}{P(\boldsymbol{\Delta}\mid\Omega_I)P(\Omega_I)+P(\boldsymbol{\Delta}\mid\Omega_E)P(\Omega_E)} \tag{10.23}$$

其中，$P(\Omega_I)$，$P(\Omega_E)$ 为先验概率，可以根据一定的实验环境估计得到。这里取内部图像差向量集和外部图像差向量集的个数相等，故令 $P(\Omega_I)=P(\Omega_E)$。$P(\boldsymbol{\Delta}\mid\Omega_I)$，$P(\boldsymbol{\Delta}\mid\Omega_E)$ 表示条件概率，服从多维正态分布。如果有足够的样本，就可以用参数估计的方法分别求出 $\boldsymbol{\Delta}$ 在这两个空间中的条件概率。这样如果 $P(\boldsymbol{\Delta}\mid\Omega_I)>P(\boldsymbol{\Delta}\mid\Omega_E)$，则判决 $\boldsymbol{I}_1$，$\boldsymbol{I}_2$ 是同一个人，否则是不同的人。

2．神经网络

一般而言，神经网络是一个并行和分布式的信息处理网络结构，它一般由许多个神经元组成，每个神经元只有一个输出，它可以连接到很多其他的神经元，每个神经元输入有多个连接通路，每个连接通路对应于一个连接权系数。

严格地说，神经网络是一个具有下列性质的有向图[27]。

（1）每个节点有一个状态变量 x_j。

（2）节点 i 到节点 j 有一个连接权值系数 w_{ij}。

（3）每个节点有一个阈值 θ_j。

（4）每个节点定义一个变换函数 $f_j(x_i,w_{ij},\theta_j(i\neq j))$，最常见的形式为：

$$f_j\left(\sum_i w_{ij}x_i-\theta_j\right) \tag{10.24}$$

有代表性的网络模型有感知器，多层影射 BP 网络、RBF 网络、Hopfield 模型等。几乎所

有神经元学习算法都可以看做 Hebb 学习规则的变形。Hebb 学习规则的基本思想是[27]：如果神经元 u_i 接收来自另一神经元 u_j 的输出，则当这两个神经元同时兴奋时，从 u_i 到 u_j 的权值就得到加强。

具体到前述的神经元模型，可以将 Hebb 规则表现为如下的算法：

$$\Delta w_{ij} = \lambda x_i y_j \tag{10.25}$$

其中，Δw_{ij} 是对第 i 个权值的修正量；λ 是控制学习速度的系数。

通常利用神经网络进行人脸识别需要考虑两方面的因素：

（1）选择人脸图像的哪些参数作为神经网络的输入；

（2）选择何种神经网络。

神经网络的输入策略有两类：

① 第一类是将提取到的特征向量作为输入向量。这些特征向量可以是由线性方法提取的特征向量，也可以是由非线性方法提取的。

② 第二类是将人脸图像像素直接输入神经网络。输入可以是全局人脸图像，也可以是经过定位的局部人脸组分图像。

第一类输入策略可以有效地控制神经网络的规模，提高神经网络的运行速度，但同时对提取特征的要求较高，提取什么特征，以及提取多少特征才能满足识别的要求很难先验得出。而第二类输入策略对于特征提取的要求降低，并可以根据样本集自身的群体特性（方差特征）来进行特征选择，但同时带来的问题是网络的规模扩大而造成收敛的缓慢及不稳定，计算量太大。所以，将全局的特征提取与人工神经网络结合起来可能会在人脸识别方面得到比较好的效果。

神经网络方法的缺点是：要求通过获得同一个人的多幅人脸图像来进行网络的学习和训练，当待测试的人脸图像类别较多时，网络学习的计算量较大，训练时间比较长。

3．最近特征线[28]

最近特征线（Nearest Feature Line，NFL）的基本思想是将模式在特征空间的表示由有限个已知特征点扩充到任意两个特征点所在的特征直线（即增加无限个虚拟特征点），以与测试样本特征点距离最近的特征直线所属的类别作为测试样本的类别。很明显，NFL 将同模式特征点之间存在的联系具体解释为所有特征直线上的新增虚拟特征点，赋予了虚拟特征点较原型特征点在分类识别中同等重要的地位。因此，NFL 是最近邻法的直线推广。

设已知由 C 类模式的特征点组成的训练集 $\{\boldsymbol{x}_{c,i} | 1 \leqslant c \leqslant C,\ 1 \leqslant i \leqslant n_c\}$（$n_c$ 为第 c 类模式的训练样本数），对于第 c 类任意两个不同的特征点，定义测试样本特征点 x 到这两点决定的特征直线 $\boldsymbol{L}_{c;i;j}$ 的距离为：

$$d(\boldsymbol{x}, \boldsymbol{L}_{c;i;j}) = \| \boldsymbol{x} - \boldsymbol{p}_{c;i;j} \| \tag{10.26}$$

其中，$\|\cdot\|$ 表示取向量的欧氏距离；$\boldsymbol{p}_{c;i;j} = \boldsymbol{x}_{c;i} + \lambda(\boldsymbol{x}_{c;j} - \boldsymbol{c}_{c;i})$ 表示 $\boldsymbol{x}$ 的类别标志 $\overline{c}$ 由最近特征直线 $\boldsymbol{L}_{\overline{c};\overline{i};\overline{j}}$ 的类别标记决定，即

$$\overline{c} = \arg d(\boldsymbol{x}, \boldsymbol{L}_{\overline{c};\overline{i};\overline{j}}) = \arg \min_{1 \leqslant c \leqslant C} \min_{1 \leqslant i, j \leqslant n_c, i \neq j} d(\boldsymbol{x}, \boldsymbol{L}_{c;i;j}) \tag{10.27}$$

为方便将 NFL 方法向高维推广，将 $\boldsymbol{p}_{c;i;j}$ 表示成另一种形式：

$$\boldsymbol{p}_{c;i;j} = \boldsymbol{x}_{c;i} + \boldsymbol{A}_{c;i;j}(\boldsymbol{A}_{c;i;j}^{\mathrm{T}} \boldsymbol{A}_{c;i;j})^{-1} \cdot \boldsymbol{A}_{c;i;j}^{\mathrm{T}}(\boldsymbol{x} - \boldsymbol{x}_{c;i}) \tag{10.28}$$

相应地，

$$d(\boldsymbol{x}, \boldsymbol{L}_{c;i;j}) = \| (\boldsymbol{E} - \boldsymbol{A}_{c;i;j}(\boldsymbol{A}_{c;i;j}^{\mathrm{T}} \boldsymbol{A}_{c;i;j})^{-1} \cdot \boldsymbol{A}_{c;i;j}^{\mathrm{T}}(\boldsymbol{x} - \boldsymbol{x}_{c;i}) \| \tag{10.29}$$

其中，$\boldsymbol{E}$ 为单位矩阵。

10.4 核机器学习在人脸识别中的应用

10.4.1 基于核机器的非线性特征选择与提取

1. 无监督方法

1）核主元分析。

核主元分析就是先用核方法将数据投影到高维特征空间 F 中，再对其做主元分析。在 F 中进行主成分分析就是求解如下的特征值问题：

$$\lambda \boldsymbol{w}^{\phi} = \boldsymbol{S}^{\phi} \boldsymbol{w}^{\phi} \tag{10.30}$$

其中，$\boldsymbol{S}^{\phi}$ 表示样本在隐特征空间 F 中投影的离散度矩阵。根据再生核理论所有对应于 $\lambda \neq 0$ 的特征向量 $\boldsymbol{w}^{\phi}$ 必然存在于 $\boldsymbol{\phi}(\boldsymbol{x}_1), \boldsymbol{\phi}(\boldsymbol{x}_2), \cdots, \boldsymbol{\phi}(\boldsymbol{x}_n)$ 所张成的空间中，于是 $\boldsymbol{w}^{\phi}$ 可以用它们的线性组合来表示：

$$\boldsymbol{w}^{\phi} = \sum_{i=1}^{n} \alpha_i \boldsymbol{\phi}(\boldsymbol{x}_i) \tag{10.31}$$

将式（10.31）代入式（10.30），就变成了下面的特征值问题：

$$n\lambda \boldsymbol{\alpha} = \boldsymbol{K} \boldsymbol{\alpha} \tag{10.32}$$

其中，$\boldsymbol{K}$ 是 $n \times n$ 的核矩阵，$K_{ij} = k(\boldsymbol{x}_i, \boldsymbol{x}_j) = <\boldsymbol{\phi}(\boldsymbol{x}_i), \boldsymbol{\phi}(\boldsymbol{x}_j)>$。选择对应于前 m 个最大特征值的特征向量作为 F 中的主元，则原空间的人脸 $\boldsymbol{x}$ 在 $\boldsymbol{w}^{\phi}$ 上的投影就是：

$$y=(\boldsymbol{w}^{\phi}\cdot\boldsymbol{\phi}(\boldsymbol{x}))=\sum_{i=1}^{n}\alpha_i k(\boldsymbol{x}_i,\boldsymbol{x}) \tag{10.33}$$

2）核典型相关分析法。

线性典型相关判别作为一种线性判别方法，和其他线性判别方法一样，分类数据非线性可分时，它的分类效果是不理想的。因此，基于核理论的思想，将典型相关的线性判别演变为非线性判别，能够使其识别能力大大提高。下面简单地描述一下它的推导过程。

和其他核方法一样，基于核理论的非线性典型相关分析首先通过一个非线性映射$\boldsymbol{\phi}(\mathbf{R}^n\rightarrow F)$将 $\mathbf{R}^n$ 中的样本映射到一个特征空间：$F:\phi(\boldsymbol{x})\in F$，然后在 F 中执行线性典型相关判别分析。基于 KCCA 的判别分析与传统 CCA 方法不同的是：KCCA 将待研究的变量分别映射到不同的特征空间。对于判别分析，将训练样本的类标变量映射到特征空间是没有意义的，因此我们采用一种不同于一般 CCA 的方法推导。

按照参考文献[29]的方法，利用人脸图像样本及其所属类别信息构造两组数据矩阵 $\boldsymbol{X}$ 和 $\boldsymbol{Y}$，用这两组数据矩阵进行 CCA 得到最佳鉴别向量 $\boldsymbol{a}$。用 CCA 进行鉴别分析只用到向量对 $\boldsymbol{a}$ 和 $\boldsymbol{b}$ 中的 $\boldsymbol{a}$，向量 $\boldsymbol{b}$ 不起作用。

设有 C 个类别 $w_1,w_2,\cdots,w_C$，第 i 类有 n_i 个样本，总样本数 $n=\sum_{i-1}^{c}n_i$，构造样本数据矩阵 $\boldsymbol{X}$：

$$\boldsymbol{X}=[\boldsymbol{x}_{11},\boldsymbol{x}_{12},\cdots,\boldsymbol{x}_{C1},\boldsymbol{x}_{C2},\cdots,\boldsymbol{x}_{Cn_C}]^{\mathrm{T}} \tag{10.34}$$

$\boldsymbol{x}_{ij}\in\mathbf{R}^d$ 为第 i 个类别中的第 j 个样本，其为 d 维的列向量。根据每个样本所属类别构造矩阵 $\boldsymbol{Y}$：

$$\boldsymbol{Y}=\begin{pmatrix}\mathbf{1}_{n_1} & \mathbf{0}_{n_1} & \cdots & \mathbf{0}_{n_1}\\ \mathbf{0}_{n_2} & \mathbf{1}_{n_2} & \cdots & \mathbf{0}_{n_2}\\ \vdots & \cdots & \ddots & \vdots\\ \vdots & \cdots & \cdots & \mathbf{1}_{n_{C-1}}\\ \mathbf{0}_{n_C} & \mathbf{0}_{n_C} & \cdots & \mathbf{1}_{n_C}\end{pmatrix} \tag{10.35}$$

式中，$\mathbf{1}_{n_i}$ 为元素全为 1 的 $n_i\times1$ 列向量；$\mathbf{0}_{n_i}$ 为元素全为 0 的 $n_i\times1$ 列向量。显然，$\boldsymbol{Y}$ 每一行对应矩阵 $\boldsymbol{X}$ 每一行的样本，指示了 $\boldsymbol{X}$ 每行样本所在类别。$\boldsymbol{Y}$ 的 1，2，…，C–1 列分别对应第 1，2，…，C–1 个类别，从而刻画了训练样本的类别信息。

为了推导出 KCCA，依据核机器学习的思想，用一个非线性映射将 $\mathbf{R}^d$ 空间中的样本 $\boldsymbol{x}$ 映射到特征空间 H，在特征空间中进行分析。样本数据矩阵 $\boldsymbol{X}$ 映射为：

$$\boldsymbol{X}_{\phi}=[\boldsymbol{\phi}(\boldsymbol{x}_{11}),\boldsymbol{\phi}(\boldsymbol{x}_{12}),\cdots,\boldsymbol{\phi}(\boldsymbol{x}_{C1}),\boldsymbol{\phi}(\boldsymbol{x}_{C2}),\cdots,\boldsymbol{\phi}(\boldsymbol{x}_{Cn_C})]^{\mathrm{T}} \tag{10.36}$$

对于判别分析，将类别信息映射到高维特征空间没有意义，因此类别信息矩阵 $\boldsymbol{Y}$ 不变。样本经非线性变换后在特征空间中的内积运算，可用满足 Mercer 条件的正定核函数 $k(\boldsymbol{x},\boldsymbol{y})$ 来代替特征空间的内积 $\boldsymbol{\phi}(\boldsymbol{x})^{\mathrm{T}}\boldsymbol{\phi}(\boldsymbol{y})$，在原空间中完成运算。用非线性变换后的样本矩阵 $\boldsymbol{X}_{\phi}$ 定义核矩阵 $\boldsymbol{K}$：

$$\boldsymbol{K}=\boldsymbol{X}_{\phi}\boldsymbol{X}_{\phi}^{\mathrm{T}} \tag{10.37}$$

$n\times n$ 对称阵 $\boldsymbol{K}$ 的第 i 行、第 j 列元素为 $K_{ij}=k(\boldsymbol{x}_i,\boldsymbol{x}_j)$。

KCCA 判别分析的目的就是求两个投影向量 $\boldsymbol{a}$ 和 $\boldsymbol{b}$，使达到如下优化：

$$\arg\max_{\boldsymbol{a},\boldsymbol{b}}\boldsymbol{a}^{\mathrm{T}}\boldsymbol{X}_{\phi}^{\mathrm{T}}\boldsymbol{Y}\boldsymbol{b} \tag{10.38}$$

其中，

$$\boldsymbol{a}^{\mathrm{T}}\boldsymbol{X}_{\phi}^{\mathrm{T}}\boldsymbol{X}_{\phi}\boldsymbol{a}=\boldsymbol{b}^{\mathrm{T}}\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{Y}\boldsymbol{b}=\boldsymbol{1} \tag{10.39}$$

由核机器学习的理论可知，所求鉴别向量 $\boldsymbol{a}$ 在所有样本 $\{\boldsymbol{\phi}(\boldsymbol{x}_i)\}(i=1,\cdots,n)$ 的张成空间中，即存在 n 维列向量 $\boldsymbol{\alpha}$，使得：

$$\boldsymbol{a}=\boldsymbol{X}_{\phi}^{\mathrm{T}}\boldsymbol{\alpha} \tag{10.40}$$

求解向量 $\boldsymbol{a}$ 只需求解列向量 $\boldsymbol{\alpha}$。

由以上公式得到约束优化问题为：

$$\max_{\boldsymbol{a},\boldsymbol{b}}(r(\boldsymbol{\alpha},\boldsymbol{b}))=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{X}_{\phi}\boldsymbol{X}_{\phi}^{\mathrm{T}}\boldsymbol{Y}\boldsymbol{b}=\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{K}\boldsymbol{Y}\boldsymbol{b} \tag{10.41}$$

其中，

$$\boldsymbol{a}^{\mathrm{T}}\boldsymbol{X}_{\phi}\boldsymbol{X}_{\phi}^{\mathrm{T}}\boldsymbol{a}=\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{K}\boldsymbol{\alpha}=\boldsymbol{b}^{\mathrm{T}}\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{Y}\boldsymbol{b}=\boldsymbol{1} \tag{10.42}$$

用拉格朗日乘数法求解上述极值问题，令 $\lambda/2$ 和 $u/2$ 为拉格朗日乘子，构造拉格朗日函数为：

$$L(\boldsymbol{\alpha},\boldsymbol{b},\lambda,u)=\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{K}\boldsymbol{Y}\boldsymbol{b}-\frac{\lambda}{2}(\boldsymbol{\alpha}^{\mathrm{T}}\boldsymbol{K}^2\boldsymbol{\alpha}-\boldsymbol{1})-\frac{u}{2}(\boldsymbol{b}\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{Y}\boldsymbol{b}-\boldsymbol{1}) \tag{10.43}$$

分别求 $L(\boldsymbol{\alpha},\boldsymbol{b},\lambda,u)$ 对 $\boldsymbol{\alpha}$ 和 $\boldsymbol{b}$ 的偏导数，并令其为 0 可得：

$$\frac{\partial L}{\partial\boldsymbol{\alpha}}=\boldsymbol{K}\boldsymbol{Y}\boldsymbol{b}-\lambda\boldsymbol{K}^2\boldsymbol{\alpha}=0 \tag{10.44}$$

$$\frac{\partial L}{\partial\boldsymbol{b}}=\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{K}\boldsymbol{\alpha}-u\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{Y}\boldsymbol{b}=0 \tag{10.45}$$

求解可得 $\lambda=u,\boldsymbol{b}=\frac{1}{u}(\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{Y})^{-1}\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{K}\boldsymbol{\alpha}$。

代入上式可得：

$$\boldsymbol{K}^{-1}\boldsymbol{Y}(\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{Y})^{-1}\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{K}\boldsymbol{\alpha}=\lambda^2\boldsymbol{\alpha} \tag{10.46}$$

求解列向量$\boldsymbol{\alpha}$只需求解此特征方程式的非零特征值对应的特征向量。

非线性变换后的训练样本需通过下式对矩阵 $\boldsymbol{K}$ 中心化[30]：

$$\widetilde{\boldsymbol{K}}=\boldsymbol{K}-\frac{1}{n}\boldsymbol{K}\boldsymbol{I}-\frac{1}{n}\boldsymbol{I}\boldsymbol{K}+\frac{1}{n^2}\boldsymbol{I}\boldsymbol{K}\boldsymbol{I} \tag{10.47}$$

其中，$\boldsymbol{I}$ 为 $n\times n$ 的单位阵。

经中心化上式变为：

$$\widetilde{\boldsymbol{K}}^{*}\boldsymbol{Y}(\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{Y})^{-1}\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{K}\boldsymbol{\alpha}=\lambda^2\boldsymbol{\alpha} \tag{10.48}$$

其中，$\widetilde{\boldsymbol{K}}^{*}$ 为 $\widetilde{\boldsymbol{K}}$ 的广义逆，矩阵 $\boldsymbol{Y}^{\mathrm{T}}\boldsymbol{Y}$ 的秩为 $C-1$，因此如果按降序排列，可得到 $C-1$ 个非零特征值 $\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_{C-1}$ 和其对应的 n 维特征向量 $\boldsymbol{\alpha}_k(k=1,2,\cdots,C-1)$。可分别求出相应的 $\boldsymbol{a}$。从而我们可以得到一个非线性的特征抽取投影方程：

$$z=(\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_{C-1})^{\mathrm{T}}\boldsymbol{X}_{\phi}\boldsymbol{\phi}(z)=(\boldsymbol{\alpha}_1,\boldsymbol{\alpha}_2,\cdots,\boldsymbol{\alpha}_{C-1})^{\mathrm{T}}\boldsymbol{K}_{\mathrm{z}} \tag{10.49}$$

其中，

$$\boldsymbol{K}=(k(\boldsymbol{x}_1,z),k(\boldsymbol{x}_2,z),\cdots,k(\boldsymbol{x}_i,z))^{\mathrm{T}}(i=1,2,\cdots,n) \tag{10.50}$$

2．有监督方法

有监督的核特征提取方法主要有核判别分析等方法。核判别分析法的主要思想如下。

经过非线性映射$\boldsymbol{\phi}$，训练样本 $\boldsymbol{\phi}(\boldsymbol{x}_i)(i=1,\cdots,n)$ 的类内散布矩阵 $\boldsymbol{S}_w^{\phi}$ 和类间散布矩阵 $\boldsymbol{S}_b^{\phi}$ 分别为：

$$\boldsymbol{S}_w^{\phi}=\sum_{i=1}^{c}\frac{n_i}{n}(\boldsymbol{m}_i^{\phi}-\boldsymbol{m}^{\phi})(\boldsymbol{m}_i^{\phi}-\boldsymbol{m}^{\phi})^{\mathrm{T}} \tag{10.51}$$

$$\boldsymbol{S}_b^{\phi}=\frac{1}{n}\sum_{i=1}^{c}\sum_{j=1}^{n_i}(\boldsymbol{\phi}(\boldsymbol{x}_j)-\boldsymbol{m}_i^{\phi})(\boldsymbol{\phi}(\boldsymbol{x}_j-\boldsymbol{m}_i^{\phi}))^{\mathrm{T}} \tag{10.52}$$

其中，$\boldsymbol{m}^{\phi}$为总体均值向量；$\boldsymbol{m}_i^{\phi}$ 为第 i 类的均值，而且，

$$\boldsymbol{m}^{\phi}=\frac{1}{n}\sum_{i=1}^{n_i}\boldsymbol{\phi}(\boldsymbol{x}_i) \tag{10.53}$$

$$\boldsymbol{m}_i^{\phi}=\frac{1}{n_i}\sum_{i=1}^{n_i}\boldsymbol{\phi}(\boldsymbol{x}_i),i=1,\cdots,C \tag{10.54}$$

则最佳投影方向为：

$$\boldsymbol{W}_{\text{opt}} = \arg\max_{\boldsymbol{w}} \left| \frac{(\boldsymbol{w}^{\phi})^{\mathrm{T}} \boldsymbol{S}_b^{\phi} (\boldsymbol{w}^{\phi})}{(\boldsymbol{w}^{\phi})^{\mathrm{T}} \boldsymbol{S}_w^{\phi} (\boldsymbol{w}^{\phi})} \right| = \left(\boldsymbol{w}_1^{\phi}, \cdots, \boldsymbol{w}_m^{\phi} \right) \tag{10.55}$$

$\boldsymbol{W}_{\text{opt}}$ 就是特征值问题：

$$\lambda \boldsymbol{S}_w^{\phi} \boldsymbol{w}^{\phi} = \boldsymbol{S}_b^{\phi} \boldsymbol{w}^{\phi} \tag{10.56}$$

的解。即所求的投影轴 $(\boldsymbol{w}_1^{\phi}, \cdots, \boldsymbol{w}_m^{\phi})$ 是式（10.55）中前 m 个最大特征值对应的特征向量。

10.4.2 基于核机器的人脸分类

1．支持向量机

支持向量机（Support Vectors Machine，SVM）是在统计学习理论基础上由 Vapnik 等人发展起来的一种新的机器学习方法。SVM 方法具有神经网络无法相比的许多优点，例如，SVM 得到的解是全局最优的，SVM 具有完整的理论体系等。在实际求解中。SVM 可表示为一个凸的二次优化求解问题。下面简要介绍一下 SVM 的求解算法。

假设 $(\boldsymbol{x}_i, \boldsymbol{y}_i), i = 1, \cdots, n, \boldsymbol{x} \in \mathbf{R}^d, y \in \{+1, -1\}$ 是类别标号。SVM 的目标是构建如下的分类器：

$$f(x) = \operatorname{sgn}(\boldsymbol{\omega} \bullet \boldsymbol{x} + b) = \operatorname{sgn}\left(\sum_{i=1}^{n} y_i \alpha_i k(\boldsymbol{x}, \boldsymbol{x}_i) + b \right) \tag{10.57}$$

其中，$\alpha_i > 0$，$b \in \mathbf{R}$，$\operatorname{sgn}(\bullet)$ 为符号函数；$k(\cdot,\cdot)$ 为核函数，实际应用中，常用核函数有如下几种。

（1）多项式核函数：$k(\boldsymbol{x}, \boldsymbol{x}_i) = [(\boldsymbol{x} \bullet \boldsymbol{x}_i) + 1]^q$，所得到的是 q 阶多项式分类器。

（2）径向基核函数：$k(\boldsymbol{x}, \boldsymbol{x}_i) = \exp(-\|\boldsymbol{x} - \boldsymbol{x}_i\|^2 / 2\sigma^2)$，所得的分类器与传统的径向基神经网络分类器的最大区别在于这里每个基函数中心对应一个支持向量，它们与输出权值都是由算法自动确定的。

（3）sigmoid 核函数：$k(\boldsymbol{x}, \boldsymbol{x}_i) = \tanh(v(\boldsymbol{x} \bullet \boldsymbol{x}_i) + c)$，这时支持向量机实现的是包含一个隐含层的多层感知器，隐含层的节点个数由算法自动确定，而且不存在困扰神经网络的局部极小点问题。

分类器式（10.57）通过下列条件构建得到：

$$\begin{cases} \boldsymbol{w}^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}_i) + b \geqslant 1, (y_i = 1) \\ \boldsymbol{w}^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}_i) + b \leqslant -1, (y_i = -1) \end{cases} (i = 1, \cdots, n) \tag{10.58}$$

等价形式为：

$$y_i[\boldsymbol{w}^{\mathrm{T}}\boldsymbol{\phi}(\boldsymbol{x}_i)+b]\geqslant 1(i=1,\cdots,n) \tag{10.59}$$

其中，$\boldsymbol{\phi}(\bullet)$ 为某非线性映射函数。

当训练样本不可分时，引入非负松弛变量 ξ_i，使得：

$$\begin{cases} y_i[\boldsymbol{w}^{\mathrm{T}}\boldsymbol{\phi}(\boldsymbol{x}_i)+b]\geqslant 1-\xi_i \\ \xi_i\geqslant 0 \end{cases}(i=1,\cdots,n) \tag{10.60}$$

根据结构风险最小化理论（Vapnik，1995），求解上式的问题可转化为求解下列二次优化问题：

$$\min_{\boldsymbol{w},\xi} J(\boldsymbol{w},\xi_i)=\frac{1}{2}\boldsymbol{w}^{\mathrm{T}}\boldsymbol{w}+C\sum\nolimits_{i=1}^{n}\xi_i \tag{10.61}$$

$$\text{s.t.}\ \begin{cases} y_i[\boldsymbol{w}^{\mathrm{T}}\boldsymbol{\phi}(\boldsymbol{x}_i)+b]\geqslant 1-\xi_i \\ \xi_i\geqslant 0 \end{cases}(i=1,\cdots,n)$$

构造拉格朗日函数：

$$L(\boldsymbol{\omega},b,\xi_i,\alpha_i,s_i)=J(\boldsymbol{\omega},\xi_i)-\sum_{i=1}^{n}\alpha_i\left\{y_i[(\boldsymbol{\omega}^{\mathrm{T}}\boldsymbol{\phi}(\boldsymbol{x}_i)+b]-1+\xi_i\right\}-\sum_{i=1}^{n}s_i\xi_i$$

其中，$\alpha_i\geqslant 0$，$s_i\geqslant 0$，$(i=1,\cdots,n)$。

于是，求解式（10.61）的优化问题转化为求解如下的优化问题：

$$\max_{\alpha_i s_i}\min_{\boldsymbol{w},b,\xi_i} L(\boldsymbol{\omega},b,\xi_i,\alpha_i,s_i) \tag{10.62}$$

求解式（10.62）的详细过程可参见参考文献[31]。

2．支持向量数据描述[32]

基于支持向量的数据描述（Support Vectors Data Description，SVDD），也称为单值分类方法或野点检测方法，可以较好地获得数据的分布区域，对异类具有良好的拒识能力，在实际应用中有非常好的分类效果。单值分类方法只需要一个单独的类，通过用传统的启发式方法在不影响识别率的情况下可以减少分类所需的训练样本[33]。SVDD 不是寻求最优的超平面而是试图找到一个体积最小的超球体（球心为 $\boldsymbol{a}$，半径为 R），使尽可能多的 $\boldsymbol{x}_i$ 都落在该球体内，而将野点（outliers）排除在球体之外，可以通过构造如下误差函数 F 来获得：

$$F(R,\boldsymbol{a})=R^2 \tag{10.63}$$

并使其最小化，且约束条件为：

$$\| \boldsymbol{x}_i - \boldsymbol{a} \|^2 \leqslant R^2, \quad \forall i \tag{10.64}$$

显然这种定义对极少数偏远的样本很敏感，会导致球的体积很大而不能较好地表示目标数据。因此允许部分样本点在球体以外，即经验误差不必为 0。

引入松弛变量$\delta_i \geqslant 0$，问题可以转化为求下面问题的最小值：

$$F(R, \boldsymbol{a}, \delta) = R^2 + c\sum_i \delta_i \tag{10.65}$$

满足如下约束条件：

$$\| \boldsymbol{x}_i - \boldsymbol{a} \|^2 \leqslant R^2 + \delta_i, \quad \delta_i \geqslant 0, \forall_i \tag{10.66}$$

c 为惩罚系数，用来控制描述的量与分类错误的折中。将式（10.66）代入式（10.65）并引入拉格朗日乘子，问题转化为求解如下拉格朗日方程的最大值：

$$L = \sum_i \alpha_i k(\boldsymbol{x}_i, \boldsymbol{x}_j) - \sum_{i,j} \alpha_i \alpha_j k(\boldsymbol{x}_i, \boldsymbol{x}_j) \tag{10.67}$$

约束条件为：

$$0 \leqslant \alpha_i \leqslant c \qquad \sum_{i=1}^{n} \alpha_i = 1 \tag{10.68}$$

其中，$k(\boldsymbol{x}_i, \boldsymbol{x}_j) = (\boldsymbol{\phi}(\boldsymbol{x}_i), \boldsymbol{\phi}(\boldsymbol{x}_j))$ （10.69）

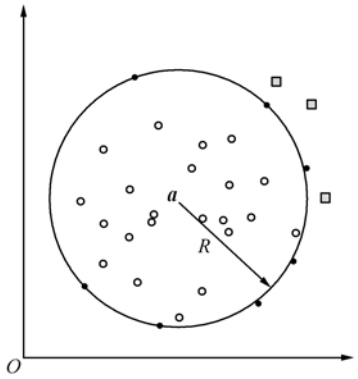


图 10.2 SVDD 中超球边界与支持向量

$\boldsymbol{a} = \sum_{i=1}^{n} \alpha_i \boldsymbol{x}_i$ 表明球体的中心是样本数据的线性组合，权重系数为 α_i。根据拉格朗日乘子的特性，$\alpha_i = 0$ 表明对应的样本点位于球体内部；$\alpha_i > 0$ 表明对应的样本点位于超球面的边界上，在图 10.2 中以“●”标记；$\alpha_i = c$ 表明对应的样本位于球体外，在图中以“□”标记。那些位于球体边界上的少数样本成为支持向量（SV），对于超球体的描述只需要这些样本就可以了。于是超球体的半径 R 可用超球面中心 $\boldsymbol{a}$ 和位于球体分界上的支持向量 $\boldsymbol{x}_k$（对应 $\alpha_k > 0$）来表示：$R^2 = k(\boldsymbol{x}_k, \boldsymbol{x}_k) - 2\sum_i \alpha_i (\boldsymbol{x}_k, \boldsymbol{x}_i) + \sum_{i,j} \alpha_i \alpha_j (\boldsymbol{x}_i, \boldsymbol{x}_j)$。

对一个新的样本 $\boldsymbol{z}$ 如果满足下式我们可以判定其为目标样本：

$$f_{\mathrm{SVDD}}(\boldsymbol{z}) = \| \boldsymbol{z} - \boldsymbol{a} \|^2 = k(\boldsymbol{z},\boldsymbol{z}) - 2\sum_i \alpha_i k(\boldsymbol{z},\boldsymbol{x}_i) + \sum_{i,j} \alpha_i \alpha_j k(\boldsymbol{x}_i,\boldsymbol{x}_j) \leqslant R^2 \tag{10.70}$$

否则，判断为非目标样本，拒绝接受。

不同的核函数在原始输入空间得到的描述边界也不相同，因此需要选择适合的核函数来建立好的柔性描述。Tax 对多项式核函数与 RBF 核函数在 SVDD 中的应用进行了比较研究，认为 RBF 核函数只与样本点之间的距离有关，而与样本点与球心的相对位置无关，更适合于得到紧凑的数据描述[33]。

3．基于 KCCA 与 SVDD 的人脸识别[29]

设 KCCA 中的核函数记为 K_1，多类分类中的核函数记为 K_2，下面给出了将改进的 KCCA 特征提取方法和 SVDD 分类器相结合的步骤。

Step 1：选择核函数 K_1，确定训练样本集的规模。

Step 2：用特征向量选择方法选择训练样本子集。

Step 3：通过 10.4.1 节计算 KCCA 的方法得到最佳投影方向矢量 $\boldsymbol{a}$，将人脸特征的投影系数作为 SVDD 分类器的输入。

Step 4：对一个新的训练样本 $\boldsymbol{z}$，通过上述方法选择其特征矢量，然后将提取到的该线性特征向量代入到训练好的多分类器中，判断其所属类别。

10.4.3　基于软计算的核函数选择与优化

1．混沌理论

混沌（Chaos）[34]是自然界广泛存在的一种非线性现象，混沌理论还远远没有成熟，到目前为止，混沌还没有一个标准的定义，但普遍认为混沌系统应该具备以下几个特征。

（1）非线性。首先，线性系统不具有混沌行为；其次，非线性并不保证有混沌。

（2）确定性。尽管系统行为表面上看起来具有随机性，但系统在将来某个时候的状态是确定的而不是随机的，我们能够按照某种规则预知系统的行为，即常说的混沌是一种貌似随机的确定性行为。

（3）对初始条件的敏感依赖性。即初始条件的微小变化能引起系统最终状态的巨大差异。很多学者都把这一点作为混沌的本质特征，而事实上很多混沌现象也是根据混沌的这一特征而发现的。

（4）貌似随机性。即无序中的有序。

2．粒子群优化算法

粒子群优化算法是由 Kennedy 和 Eberhart 在 1995 年提出的一种基于群体智能（Swarm Intelligence）的进化计算技术[35]。在 PSO 模型中，每个优化问题的解就是搜索空间中的一个粒子。粒子在搜索空间中以一定的速度飞行，这个速度根据它本身的飞行经验和群体的飞行经验来动态调整。设 $X_i=(x_{i1},x_{i2},\cdots,x_{in})$ 表示粒子 i 当前在解空间中的位置，并由评价函数计算其适应度，$V_i=(v_{i1},v_{i2},\cdots,v_{in})$ 表示粒子 i 的当前飞行速度，决定它们运动的方向和距离，然后粒子们就追随当前的最优粒子在解空间中搜索。

首先初始化一群随机粒子，然后通过迭代找到最优解，在每一次迭代中，粒子通过跟踪两个“极值”来更新其速度和位置。第一个极值就是粒子本身所找到的最优解，叫做个体极值 p_{best}；第二个极值是粒子种群目前找到的最优解，叫全局极值 g_{best}。粒子根据以下公式来更新其速度和位置：

$$V_i(k+1)=\omega V_i(k)+c_1\text{Rand}(p_{\text{best}}-X_i(k))+c_2\text{Rand}(g_{\text{best}}-X_i(k)) \tag{10.71}$$

$$X_i(k+1)=X_i(k)+V_i(k+1) \tag{10.72}$$

其中，ω为惯性权重；k 为迭代次数；c_1、c_2 为学习因子，一般的取值在 1.5～2 之间；Rand 为均匀分布在 0～1 之间的随机数。p_{best} 是当前粒子的历史最优位置；g_{best} 是整个粒子群的历史最优位置。搜索时，粒子的位置受最大、最小位置限制，如果粒子的位置超出所给的范围，则粒子的位置将被限制为最大位置 $X_{\max}$ 或最小位置 $X_{\min}$。粒子的速度也是一样的。

基本粒子群算法由于简单、容易实现、收敛速度快等优点, 发展非常快，且成功地运用于很多领域，但由于它在搜索过程中粒子的搜索空间是一个有限的区域，不可能覆盖整个空间，因此基本粒子群算法不能保证以概率为 1 收敛到全局最优解，且容易陷入早熟收敛[36]。

3．混沌粒子群优化算法

利用混沌运动的遍历性和对初始条件的敏感性对粒子群算法进行改进，克服粒子群算法陷入早熟收敛的缺点。具体算法如下。

Step1：初始化种群。设种群规模为 N，粒子维数为 D，赋给混沌方程 Logistic 映射：$X_{n+1}=\mu X_n(1-X_n)$，i 个微小差异的初值即可得到 i 个混沌变量 x_i，将这 i 个变量映射到位置变量取值区间$[X_{\min},X_{\max}]$上，生成位置变量。按同样的方法生成速度变量。

Step 2：计算每个粒子的适应度值。

Step 3：将每个粒子的个体极值 p_{best} 设为当前位置，选择适应度最好的粒子所对应的个体极值作为最初的全局极值 g_{best}。

Step 4：根据式（10.71）和式（10.72）更新粒子的速度和位置。

Step 5：将每个粒子的适应度值与其 p_{best} 的值做比较，若优，更新 p_{best}，否则保留原值；在 p_{best} 中选择适应度最优的个体设为 g_{best}。

Step 6：判断是否满足收敛条件，若满足则结束优化，输出结果；否则返回 Step 2。

4．基于混沌粒子群的支持向量机参数选择

基于以上混沌粒子群优化算法，建立 SVM 参数选择模型，以径向基函数为例，需要优化的参数有函数拟合误差的大小ε、惩罚函数 C 和核参数γ。

首先定义适应度函数，取能直接反映 SVM 性能的均方差：

$$\text{MSE}=\frac{1}{n}\sum_{i=1}^{n}(y-f(x))^2 \tag{10.73}$$

其中，n 为样本个数，y 为参考模型，$f(x)$为 SVM 回归。对参数优化选择具体步骤如下。

Step 1：初始化粒子群ε、C、γ，确定群体规模 m，确定学习因子 c_1 和 c_2，随机产生各粒子的初始速度 $V_i=(v_{i1},v_{i2},\cdots,v_{in})$。

Step 2：将每个粒子的个体极值位置设置为当前位置，计算每个粒子的适应度，取适应度最好的粒子所对应的个体极值作为最初的全局极值。

Step 3：根据式（10.71）、式（10.72）更新粒子的当前速度和位置。

Step 4：对所有最优位置进行混沌优化，保证遍历所有位置。

Step 5：由式（10.73）评价每个粒子的适应度值。

Step 6：更新每个粒子的个体最优值 p_{best} 和全局最优值 g_{best}。

Step 7：若达到最大迭代次数或解不再变化就终止迭代，否则返回到 Step 3。

10.5　小结

人脸识别技术具有比其他生物特征识别方法更好的隐蔽性和适用性，在经济、安全、社会保障、犯罪、军事等领域都具有广泛的应用价值。

人脸识别就是利用智能信息处理技术，从包含人脸的静止图像或动态视频序列图像中提取人脸的个性特征，并以此自动识别出人的身份。其中，如何有效地提取和识别每个人脸特征，是人脸识别研究的关键问题。目前为止，还没有一种简单的方法可以使人脸特征提取与识别达到非常好的效果（具有较高的识别率和可靠度），现有的方法都有各自的优缺点和不同的适用范围。

近年来，虽然人脸识别研究领域出现了许许多多令人鼓舞的成果，然而，FRVT 2002 的

测试结果表明，光照的变化使人脸识别正确率从 90%下降到 50%。此外，人脸还会由于姿态、表情及年龄等因素的变化而呈现多变的特性。因此，如何解决光照、姿态、表情及年龄等因素的变化对人脸识别的影响问题仍然是人脸识别研究的重点之一。此外，三维人脸识别在表情变化方面体现出来的鲁棒性也得到了越来越多的关注。

参 考 文 献

[1] J.H. Friedman. Regularized discriminant analysis. Journal of the American Statistical Association, 1989, 84(405)：165-175.

[2] 王卫东，杨静宇. 采用虚拟训练样本的二次判别分析方法.自动化学报，2008，34(4)：400-407.

[3] J. P. Ye, T. Wang. Regularized discriminant analysis for high dimensional, low sample size data. Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, 2006：454-463.

[4] C.F.Song, B.C.Yin, Y.F.Sun. Eyeglasses Eigenface Based Glasses-face Recognition. Proceedings of IEEE International Conference on Networking, Sensing and Control, 2008：1385-1390.

[5] Q. S. Liu, H. Q. Lu, et al. Improving kernel Fisher discriminant analysis for face recognition. IEEE Transactions on Circuits and System for Video Technology, 2004, 14(1)：42-49.

[6] R. Epstein, P.W Hallinan, A.L. Yuille. 5 ± 2 Eigenimages suffice：an empirical investigation of low-dimensional lighting models. In IEEE Workshop on Physics-Based Modeling in Computer Vision, 1995：108-116.

[7] A. Shashua, T. Riklin-Raviv. The quotient image：class-based re-rendering and recognition with varying illuminations. IEEE Transactions on Pattern Analysis and Machine Intelligence，2001，23 (2)：129-139.

[8] Y. Wang, X. Ning, C. Yang, Q. Wang. A method of illumination compensation for human face image based on quotient image. Information Sciences, 2008, 178 (12)：2705-2721.

[9] A. Gyaourova, G. Bebis, I. Pavlidis. Fusion of infrared and visible images for face recognition. Lecture Notes in Computer Science, 2004：456-468.

[10] R. Singh, M. Vatsa, A. Noore. Hierarchical fusion of multi-spectral face images for improved recognition performance. Information Fusion, 2008, 9(2)：200-210.

[11] R. Singh, M. Vatsa, A. Noore. Intelligent biometric information fusion using support vector machine. Studies in Fuzziness and Soft Computing, 2007：325-349.

[12] F. Tsalakanidou, S. Malassiotis, MG. Strintzis. Face localization and authentication using color and depth images. IEEE Transations on Image Process, 2005, 14(2)：152-168.

[13] Chang, K.I, Bowyer, K.W, Flynn, P.J. Multiple nose regions matching for 3D face recognition under varying facial expression. IEEE Trans. PAMI, 2006, 28 (10)：1695-1700.

[14] X. Lu, AK. Jain. Deformations modeling for robust 3D face matching. 2006 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2006：1377-1383.

[15] G. Passalis, IA. Kakadiaris, T. Theoharis, G. Toderici, N. Murtuza. Evaluation of 3D face recognition in the presence of facial expressions：An annotated deformable model approach. In：Proc. FRGC Workshop, 2005：171-179.

[16] I.A. Kakadiaris, G. Passalis, G. Toderici，et al. Three-dimensional face recognition in the presence of facial expressions：An annotated deformable model approach. IEEE Trans. PAMI ,2007, 29 (4)：640-649.

[17] AM. Bronstein, MM. Bronstein, R. Kimmel. Expression-invariant representations of faces. IEEE Transactions on Image Process, 2007, 16 (1)：188-197.

[18] I. Mpiperis, S. Malassiotis, MG. Strintzis. 3-D face recognition with the geodesic polar representation. IEEE Transactions on Information Forensics and Security，2007, 2 (3)：537-547.

[19] 李盛阳. 基于视频的人脸识别研究. 华南理工大学博士学位论文，2004.

[20] Biuk Z, Loncaric S. Face recognition from multi-pose image sequence. Proceedings of the 2nd International Symposium on Image and Signal Processing and Analysis, 2001：319-324.

[21] Li Baoxin, R Chellappa. Simultaneous tracking and verification via sequential posterior estimation. Proceedings. IEEE Conference on Computer Vision and Pattern Recognition. 2000：110-117.

[22] Krüger V, Zhou Shaohua. Exemplar-based face recognition from video. Proceedings. Fifth IEEE International Conference on Automatic Face and Gesture Recognition, 2002：175-180.

[23] 孙宁，邹采荣，赵力. 人脸检测综述. 电路与系统学报，2006, 11(6)：101-113.

[24] 陈锻生，刘政凯. 肤色检测技术综述. 计算机学报，2006，29(2)：194-207.

[25] H. Yu, J. Yang. A direct LDA algorithm for high-dimensional data-with application to face

recognition. Pattern Recognition, 2001, 34(10)：2067-2070.
[26] 王静．基于贝叶斯的人脸识别．郑州大学硕士学位论文，2006.
[27] 杨梦宁. 基于非线性特征抽取法和人工神经网络的人脸识别方法的研究. 重庆大学硕士学位论文，2005.
[28] 谷秋波，武妍，王守觉，朱君波．原点无关最近特征分类器及在人脸识别的应用. 同济大学学报（自然科学版），2006，34(10)：1398-1402.
[29] Ming Li,Yuanhong Hao.Fast KCCA：A Novel Feature Extraction Method for Face Recognition. Journal of Computational Information Systems，2008，4（5）：2045-2050.
[30] 贺云辉，赵立，邹采荣．一种基于 KCCA 的小样本脸像鉴别方法．应用科学学报，2006，24(2)：140-144.
[31] AJ. Smola, B.Scholkopf, KP. Muller. The connection between regularization operators and support vector kernels. Neural Networks, 1998, 11(4)：637-649.
[32] Ming Li,Yuanhong Hao. Accelerated Kernel CCA plus SVDD：A Three-stage Process for Improving Face Recognition. Journal of Computers, 2008,3（10）：94-100.
[33] David M. J. Tax, Robert P. W. Duin. Support Vector Data Description. Machine Learning. 2004：45-66.
[34] C. M. Ou. Design of block ciphers by simple chaotic functions. IEEE Computational Intelligence Magazine, 2008, 3(2)：54-59.
[35] J. Kennedy, R. Eberhart. Particle swarm optimization. Proceedings of IEEE International Conf. on Neural Networks, Perth, Australia,1995：1942-1948.
[36] 柯晶, 钱积新, 乔谊正. 一种改进粒子群优化算法（A modified particle swarm optimization algorithm）. 电路与系统学报，2005，8 (5)：8-11.

Chapter 11

第 11 章 说话人识别

11.1 概述

11.1.1 说话人识别的研究背景

随着生物学和信息科学的高度发展，生物认证技术以其独有的稳定性、经济性、不易丢失等优点得到了广泛而深入的研究和应用。生物认证技术是根据人体自身的生理特征（指纹、手行、脸部、虹膜）和行为特征（声音、签名）来识别身份的技术，它是集光学、传感技术、红外扫描和计算机技术于一体的第三代身份验证技术，能满足现代社会对于身份鉴别的准确性、安全性与实用性的更高要求。信号检测与处理、模式识别、人工智能、机器学习等理论与技术迅速发展更进一步地推动了生物认证技术的向前发展。

说话人识别（Speaker Recognition，SR）技术是生物认证技术的重要分支，它是从说话人的一段语音中提取说话人的个性特征，通过对这些个性特征的分析和识别，从而确定或鉴别说话人的身份[1]。由于说话人发声器官的生理差异及后天形成的行为差异，每个人的语音都带有个人色彩，这使得通过分析语音信号来识别说话人成为可能。说话人识别技术以其独特的方便性、经济性和准确性等优势，日益成为人们日常生活和工作中的重要且普及的身份验证方式，有着广阔的市场应用前景。通过说话人识别技术，可以利用人本身的生物特性进行身份鉴别，例如，为公安部门进行语音验证、为一般用户提供防盗门开启等功能。在互联网

应用及通信领域，SR 技术可以应用于诸如声音拨号、电话银行、电话购物、数据库访问、信息服务、语音 E-mail、安全控制、计算机远程登录等领域。在呼叫中心应用上，说话人识别技术同样可以提供更加个性化的人机交互界面，当顾客以电话方式对呼叫中心进行请求时，系统能够根据话音判断出来者的身份，从而提供更个性化、更贴心的服务。

11.1.2 说话人识别的研究现状

说话人识别的研究主要分为两个阶段，人工说话人识别和自动说话人识别。人工说话人识别始于 20 世纪 60 年代。Bell 实验室 LGKersta 在 1962 年研究了通过可见的语谱图（Spectrogram）进行人工说话人识别，并声称在 12 个人的系统上得到了极好的识别性能，并将语谱图称为声纹（Voiceprint）。随着计算机技术的飞速发展，从 70 年代起开始进入自动说话人识别研究阶段。

Pruzansky 和 Mathews[2]于 1964 年利用模式匹配和概率统计方差分析的方法进行说话人识别研究，并提出了有名的衡量说话人特征参数有效性的 *F* 比值公式。

70 年代末期说话人识别技术获得了突破性的发展。在特征参数方面，B.S.Atall 最早在 70 年代中期就开始对说话人语音特征参数如 LPC 系数、声道的冲激响应、自相关系数、声道面积函数及倒谱系数等进行研究，并对各种参数在自动说话人识别系统中的有效性进行了验证。在识别算法方面，动态时间规整技术（Dynamic Time Warping ，DTW）基本成熟，并提出了矢量量化（Vector Quantization ，VQ）和隐马尔可夫模型（Hidden Markov Model，HMM）理论。Furui S.将 DTW 技术成功应用于说话人确认系统[3]，并且得到了较好的识别性能。同时，Rosenberg 和 Soong[4]用 VQ 进行了孤立数字文本的声纹识别研究，实验结果表明该方法的识别精度较高，且判断速度快。

进入 80 年代，经过 AT&T Bell 实验室的 Rabiner 等科学家的不懈努力，将原本艰涩的 HMM 纯数学模型工程化，使得更多研究者了解和认识了参数模型。1982 年 Poritz[5]等人将隐马尔可夫模型应用到说话人识别研究中，极大地推动了自动说话人识别技术的发展。与此同时，高斯混合模型（Gaussian Mixture Model，GMM）和人工神经网络（Artificial Neural Network，ANN）也有了较为深入的发展。ReynoldS 和 Rose[6]研究了基于高斯混合模型的说话人识别，并采用期望最大（Expectation Maximization，EM）算法来估计模型参数。高斯混合模型说话人识别是目前最为流行的与文本无关的说话人识别模型。Christopher N.等人[7]最早将 ANN 应用于自动说话人识别系统，并结合离散哈特利变换（Discrete Hartley Transform，DHT）进行特征向量的提取，获得了较高的识别性能。Oglesby 和 Mason 等人[8]研究了人工神经网络在说话人识别中的应用，提出了用径向基函数（Radial Basis Function，RBF）进行说话人识别。随着参数模型的发展，语音特征参数从以前的线性预测系数（Linear Prediction Coefficient，LPC）、

自相关系数等发展到 Mel 频率参数和基于感知线性预测（Perceptual Linear Prediction，PLP）分析提取的感知线性预测倒谱，它们在一定程度上模拟了人耳对语音的处理特点，应用了人耳听觉感知方面的一些研究成果，可以使用多元高斯分布函数[9]建模。Erell 和 Weintraub[10]在 1993 年通过实验验证了语音的倒谱特征相比其他语音参数，在干净语音和噪声环境下都能有效地提高说话人识别的识别性能。Mel 频率倒谱系数（Mel Frequency Cepstrum Coefficient，MFCC）是目前应用最为普遍的一种语音参数。它将频谱系数转换到倒谱域，使用离散余弦变换（Discrete Cosine Transform，DCT）移除邻近系数的相关性。

如今，说话人识别技术已在国内外获得了广泛的应用研究。AT&T 公司应用说话人识别技术研制出了智慧卡，已应用于自动提款机中。欧洲电信联盟 1998 年完成了 CAVE 计划，并于同年启动了 PICASSO 计划，在电信网上完成了说话人识别。同年，Motorola 和 Visa 等公司成立了 V-commerce 联盟，希望实现电子交易的自助化。其中，通过声音确定人的身份是此项目的重要组成部分。英国 Aculab 公司在 SpeechTek2002 上隆重发布其最新的声纹鉴别软件 SVI（Speaker Verification and Identification），它是第一个由语音板卡制造商自主开发、提供，而并非依赖第三方的声纹鉴别软件。其他的一些商用系统还包括：ITT 公司的 SpeakerKey，Keyware 公司的 VoiceGuardian，T-NETIX 公司的 SpeakEZ 等。

我国语音识别研究工作一直紧跟国际水平，国家对其也很重视，并把大词汇量语音识别的研究列入“863”计划，由中科院声学所、自动化所及北京大学等单位研究开发。由中国科技大学和科大讯飞公司联合建立的科大讯飞语音联合实验室，在“2008 NIST（National Institute of Standards and Technology）Speaker Recognition Evaluation”——国际说话人识别赛上，科大讯飞语音实验室送评的识别系统获得综合指标第一名的优异成绩。这表明中国在说话人识别技术上也已取得了国际领先成果。鉴于中国未来庞大的市场，国外也非常重视汉语语音识别的研究。美国、新加坡等地聚集了一批来自大陆、中国台湾、中国香港等地的学者，研究成果已达到相当高的水平。因此，国内的研究单位不仅要加强理论研究，更要加快从实验仿真系统到商品的转化。

11.1.3　说话人识别的系统结构及分类

1．说话人识别的系统结构

图 11.1 给出了说话人识别系统框图。建立和应用这一系统可以分为两个阶段，即训练阶段和识别阶段。训练阶段，系统的每个说话人说出若干训练语句，对这些训练语句进行数字化处理，提取特征向量，系统据此建立每个使用者的模板或模型参数。识别阶段由待测说话人的语音经特征提取后与系统训练时产生的每一个人的参考模型进行比较，并把与它距离最

近的那个参考模型所对应的待测者辨认为是发出输入语音的说话人。

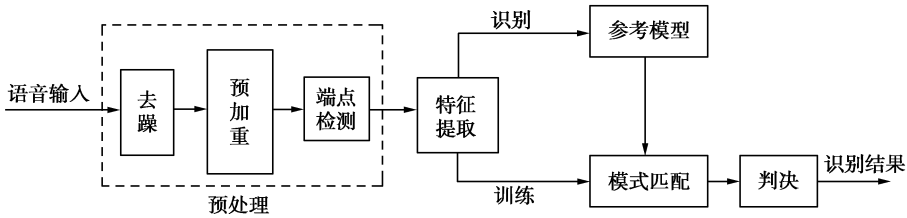


图 11.1 说话人识别系统框图

2．说话人识别的分类

说话人识别根据实现的任务不同，可分为说话人辨认（Speaker Identification）和说话人确认（Speaker Verification）两种类型[11]。说话人辨认是指对于说话人的集合 S，根据一个未知说话人的语音 x，判断 x 是否是集合 S 中的元素，以及是 S 中的哪一个元素。由此可见，说话人辨认是一个多选一的问题。而说话人确认是指验证一个人是否与他，（她）宣称的身份相符。其判断结果只有接受（accept）和拒绝（reject）两种，属于二选一的问题。

说话人识别根据系统对待识别语音内容的不同，可分为与文本有关（text-dependent）和与文本无关（text-independent）两种方式。其中与文本有关又称为固定文本（fixed text），它要求待识别的说话人按规定的内容发音，与文本无关又称为任意文本（free text），即用来识别的语音内容可以是任意的。

11.2 说话人识别中的特征参数

11.2.1 特征参数的评价方法

1．F 比

在给定了一种识别方法后，识别的效果主要取决于特征参数的选取。对于某一维单个的参数而言，可以用 F 比来表征它在说话人识别中的有效性。同一说话人的不同语音会在参数空间映射出不同的点，若对同一个人这些点分布比较集中，而对不同说话人的分布相距较远，则选取的参数就是有效的。可以选取两种分布的方差之比（F 比）作为有效性准则[12]。

$$F=\frac{\text{同一个说话人特征方差的均值}}{\text{不同说话人特征参数均值的方差}}=\frac{<[\mu_i-\bar{\mu}]^2>}{<[x_a^{(i)}-\mu_i]^2>_{a,i}} \tag{11.1}$$

这里 F 比大表示有效，即不同说话人的特征量的均值分布的离散程度分布得越散越好；而同一个说话人的分布越集中越好。式中，$<\cdot>_i$ 是指对说话人做平均，$<\cdot>_a$ 是指对某个说话人各次的某语音特征做平均，$x_a^{(i)}$ 为第 i 个说话人的第 a 次语音特征。$\mu_i=<x_a^{(i)}>_a$ 是第 i 个说话人的各次特征的估计平均值，而 $\bar{\mu}=<\mu_i>_i$ 是将所有的 μ_i 平均所得的均值。

需要说明的是，在 F 比的定义过程中假定差别分布是正态分布的，这是基本符合实际的。虽然 F 比不能直接得到误差概率，但是 F 比越大误差概率越小。因此，F 比可以作为所选特征参数的有效性准则。

2．可分性测度（D 比）

对于多维特征向量 $\boldsymbol{X}$，定义说话人内（Within speaker）特征的协方差矩阵 $\boldsymbol{W}$ 和说话人间（Between speaker）特征的协方差矩阵 $\boldsymbol{B}$ 分别为[13]：

$$\boldsymbol{W}=<(\boldsymbol{x}_a^i-\boldsymbol{\mu}_i)^{\mathrm{T}}(\boldsymbol{x}_a^i-\boldsymbol{\mu}_i)>_{a,i} \tag{11.2}$$

$$\boldsymbol{B}=<(\boldsymbol{\mu}_i-\bar{\boldsymbol{\mu}})^{\mathrm{T}}(\boldsymbol{\mu}_i-\bar{\boldsymbol{\mu}})>_i \tag{11.3}$$

其中，$\boldsymbol{\mu}_i$ 和 $\bar{\boldsymbol{\mu}}$ 意义同 F 比中相同，只是对于多维特征得到的是向量。定义可分测度（或 D 比）为：

$$\begin{aligned}D&=<(\boldsymbol{\mu}_i-\bar{\boldsymbol{\mu}})^{\mathrm{T}}\boldsymbol{W}^{-1}(\boldsymbol{\mu}_i-\bar{\boldsymbol{\mu}})>_i\\&=T_r[\boldsymbol{W}^{-1}<(\boldsymbol{\mu}_i-\bar{\boldsymbol{\mu}})^{\mathrm{T}}(\boldsymbol{\mu}_i-\bar{\boldsymbol{\mu}})>_i]\\&=T_r[\boldsymbol{W}^{-1}\boldsymbol{B}]\end{aligned} \tag{11.4}$$

其中，$T_r[\cdot]$ 是求矩阵的迹。

11.2.2　说话人识别系统中常用的特征参数

根据参数的稳定性，可把说话人特征参数大致分为两类：一类是反映说话人生理结构的固有特征，如声道结构等。这类特征主要表现在语音的频谱结构上，包含了反映声道共振的频谱包络特征信息和反映声带振动等音源特性的频谱细节构造特征信息。具有代表性的特征参数有基音和共振峰，这类特征不易被模仿，但容易受健康状况的影响。另一类是反映声道运动的动态特征，即发音方式、发音习惯等，主要表现在语音频谱结构随时间的变化上，包含了特征参数的动态特性，这类特征相对稳定但比较容易模仿，代表性的特征参数是倒谱

系数。

1．线性预测倒谱系数

线性预测倒谱系数（Linear Prediction Cepstrum Coefficient，LPCC）是一种比较重要的特征参数，它能够比较彻底地去除语音产生过程中的激励信息，能较好地描述语音信号的共振峰特性。在实际计算中，LPCC 不是由信号直接得到的，而是由线性预测参数（Linear Prediction Coefficient，LPC）求得的。LPCC 系数 $c_{L_p}(n)$ 与 LPC 系数 $a_i(i=1,2,\cdots,p)$ 之间的关系如下：

$$\begin{cases} c_{L_p}(1)=a_1 \\ c_{L_p}(n)=\sum_{k=1}^{n-1}\frac{k}{n}a_{n-k}c_{L_p}(k)+a_n,(1<n\leqslant p) \\ c_{L_p}(n)=\sum_{k=1}^{n-1}\frac{k}{n}a_{n-k}c_{L_p}(k), \qquad (n>p) \end{cases} \tag{11.5}$$

当 LPCC 系数个数不大于 LPC 系数个数时用上式中的第 2 式，当 LPCC 系数个数大于 LPC 系数个数时，用上式中的第 3 式进行计算。

2．Mel 频率倒谱系数

Mel 频率表达了一种常用的从语音频率到“感知频率”的对应关系，这更符合人耳的听觉特性，表达式为 $f_{\text{Mel}}=2595\lg(1+f/700)$。

Mel 频率倒谱系数（Mel Frequency Cepstrum Coefficient，MFCC）是将信号的频谱，首先在频域将频率轴变换为 Mel 频率刻度，再变换到倒谱域得到的倒谱系数。具体的计算过程如下。

（1）将信号进行短时傅里叶变换得到其频谱。

（2）求它的频谱幅度的平方，即能量谱，并用一组三角形滤波器在频域对能量谱进行带通滤波。

（3）将滤波器组的输出取对数，然后对它做离散余弦变换（DCT）得到 MFCC 系数。

$$\text{MFCC}_n=\sqrt{\frac{2}{N}}\sum_{k=1}^{M}\log_2 X(k)\cos[\pi(k-0.5)n/M],n=1,2,\cdots,L$$

这里 MFCC 系数的个数 L 通常取 12～16。在谱失真测度定义中通常不用 0 阶倒谱系数，因为它是反映频谱能量的。

3．其他特征参数

1）基音周期

在人的发音模型中，产生浊音周期激励脉冲的周期称为基音周期（pitch）。只有浊音才有基音周期，清音没有基音周期。基音周期检测方法大体上可分为 3 类：时域方法，频域方法和综合利用信号时域、频域特性的方法。时域方法直接利用语音信号的采样点计算信号的波峰、波谷和过零率等；频域方法主要是计算信号的自相关函数、功率谱和最大似然函数等，其精度要高于时域方法。

2）短时能量与短时平均幅度

信号 $\{x(n)\}$ 的短时能量定义为：$E_n = \sum_{m=-\infty}^{+\infty} [x(m)w(n-m)]^2$，其中 $w(n)$ 是窗函数，一般用矩形窗或汉明窗。短时能量代表的是一个语音段的语音信号的能量，可反映语音信号随时间的幅度变化。语音信号的短时平均幅度定义为：$M_n = \sum_{m=-\infty}^{+\infty} |x(m)|w(n-m)$，使用信号绝对值来代替平方和。

3）短时平均过零率

信号 $\{x(n)\}$ 的短时平均过零率定义为：$Z_n = \sum_{m=-\infty}^{+\infty} |\mathrm{sgn}[x(n)] - \mathrm{sgn}[x(n-1)]|w(n-m)$，$Z_n$ 反映了一个语音段的语音信号的过零情况，它是信号频率的一个简单量度。

11.3　说话人识别的主要方法

11.3.1　矢量量化法（VQ）

矢量量化的基本原理是将若干个标量数据组成一个矢量（或者是从一帧语音数据中提取的特征矢量）在多维空间给予整体量化，从而可以在信息量损失较小的情况下压缩数据量。

矢量量化是由标量量化推广和发展而来的一种信源编码技术。标量量化是对信号的单个样本或单个参数的幅度进行量化。这里“标量”是指被量化的变量为一维变量。矢量量化的过程是：将语音信号波形的 K 个样点的每一帧，或者有 K 个参量的每一参数帧，构成 K 维空间中的一个矢量，然后对这个矢量进行量化。通常所说的标量量化，也可以说就是 K=1 的一维矢量量化。矢量量化与标量量化相似。在标量量化时，在一维的零至无穷大值之间设置若

干个量化阶梯，当某个输入信号的幅度值落在某相邻的两个量化阶梯之间时，就被量化为两阶梯的中心值。而在矢量量化时，则将 K 维无限空间划分为 M 个区域边界，然后将输入矢量与这些边界进行比较，并被量化为“距离”最小的区域边界的中心矢量。

量化区间对应于胞腔（Voronoi cell），胞腔是多维空间中的一个区域，量化值则对应于量化矢量，它是各个胞腔的形芯。设矢量维数为 K，则 N 个胞腔各有一个 K 维的量化矢量，即 $\boldsymbol{y}_1, \boldsymbol{y}_2, \cdots, \boldsymbol{y}_i, \cdots, \boldsymbol{y}_N \in \mathbf{R}^K$。量化矢量也称为码字，这 N 个码字的集合则称为一个码本。显然，对于编码输出为 b 比特二进制数的矢量量化器，其码本大小为 $N = 2^b$,即码本为：

$$Y_N = \{\boldsymbol{y}_i, i = 1, 2, \cdots, N\}$$

如前所述，标量量化是对逐个样值的量化，矢量量化则是将每 K 个样点分为一组进行联合的多维量化处理。因而，在数学上可看做是下列 K 维信号空间上的映射，而在物理上则可看做是相应信号空间上的变换，即：

$$Q^k : \boldsymbol{X} = (X_1, \cdots, X_K) \in \mathbf{R}^K \rightarrow \boldsymbol{X}^t = (X_1^t, \cdots, X_k^t) \in \mathbf{R}^K$$

其中，$\boldsymbol{X} = (X_1, \cdots, X_K)$ 是信源 K 维欧氏空间一个连续量，$\boldsymbol{X}^t = (X_1^t, \cdots, X_K^t)$ 则是 K 维欧氏空间一个离散化矢量。

虽然采用标量量化方法也可以对矢量信号各个分量分别进行量化处理，但是采用 VQ 方法将矢量看做整体来对待，具有标量无法比拟的优越性。VQ 能有效地去除信号的冗余度，因为它能利用矢量信号的以下性质：

（1）矢量信源多维概率密度函数的形状或概率分布；

（2）信源所有矢量的各分量之间的线性相关性和统计不独立性；

（3）多维空间中胞腔的性状的多变性；

（4）多维矢量的失真测度与主观感觉的密切联系。

当利用矢量量化技术时，设计一个好的码本很重要。其关键是如何划分 N 个区域边界。这需要用大量的输入信号矢量，经过统计实验才能确定。这个过程称为“训练”或“学习”，它的任务是建立码本。它应用聚类算法，按照一定的失真准则，对训练数据进行分类，从而把训练数据在多维空间中划分成一个个以形芯（码字）为中心的胞腔，常用 LBG 算法来实现。

11.3.2 隐马尔可夫模型（HMM）

前面基于模板匹配（VQ）的算法在早期的与文本有关的说话人识别的研究中占主导地位。后来，研究人员提出了灵活性更大的随机模型，它能获得更有理论意义的可能值。利用随机模型，可以通过计算观测值的可能性来系统陈述模式识别问题。观测是指从某一说话人上提取特征向量，该向量取决于不同说话人的条件概率密度函数，该函数可以从训练矢量中估计得到。在给出了估计的概率密度函数后，概率值就可以确定了。通过这一模型，说话人的每

一帧（或是一组帧的平均值）的概率就可以计算得到，这个概率就称为匹配值。

HMM 方法给定随机模型 λ_i，然后通过计算产生一个观察 $\boldsymbol{o}_t$（来自某说话人矢量集中的一个矢量），其似然概率为 $P(\boldsymbol{o}_t|\lambda_i)$。随机模型为从说话人训练语音得到的特征矢量估计出的概率密度函数。每个说话人训练出一个随机模型。给定随机模型 λ_i 后，各说话人产生观察 $\boldsymbol{o}_t$ 的概率即被确定。当获得由某测试人产生的观察集 $\boldsymbol{o}_T$ 时，则可计算出各个随机模型以产生 $\boldsymbol{o}_T$ 的概率值 $p(\boldsymbol{o}_T|\lambda_i)$，其表示该测试语音属于已知说话人的概率值，从而做出判决。

HMM 应用到说话人识别系统时经常会遇到 3 大基本问题：① 若有 1 个 HMM 系统，对于给定的观察序列 $\boldsymbol{o}$，如何调整模型 $\boldsymbol{\lambda}=(\pi,\boldsymbol{A},\boldsymbol{B})$ 中的各要素，使概率 $p(\boldsymbol{o}|\lambda)$ 取最大值；② 已知 1 个 HMM 系统的 3 项特征参数，给定观察序列 $\boldsymbol{o}$，如何计算概率 $p(\boldsymbol{o}|\lambda)$；③ 已知 1 个 HMM 系统的 3 项特征参数，若得到了该系统产生的观察序列 $\boldsymbol{o}$，如何确定一个合理的状态序列 S，使之能最佳地产生观察序列 $\boldsymbol{o}$。上面 3 个问题的解决方案即为著名的 HMM 三大基本算法：前向_后向算法、Viterbi 算法和 Baum_Welch 算法。

11.3.3　高斯混合模型（GMM）

1．高斯混合模型（GMM）识别原理

估计得到的概率密度函数可以分为参数型和无参数型两类。如果模型是参数型的，就先提出一个概率密度函数，从而计算该密度函数的极大似然估计量。如果不知道概率密度函数，那就通过 GMM 来近似或用无参数估计来计算匹配值。每一个说话人的语音特征在特征空间中都形成了特定的分布，可以用这一分布来描述说话人的个性。高斯混合模型（GMM）是用多个高斯分布的线性组合近似说话人的特征分布，识别是将最能够产生测试音特征的说话人分布模型对应的说话人作为识别结果的。

在 GMM 中，每一个说话人的概率密度函数的函数形式是相同的，所不同的只是函数中的参数。K 阶高斯混合模型 GMM 用 K 个单高斯分布的线性组合来描述语音特征在特征空间中的分布，即：

$$p(\boldsymbol{x}\,|\,\boldsymbol{M},\theta)=\sum_{i=1}^{K}p_i b_i(\boldsymbol{x}) \tag{11.6}$$

其中，M 表示某个说话人的模型，K 为高斯混合模型的阶数，p_i 是混合权值，且 $\sum_{i=1}^{K}p_i=1$，$b_i(\boldsymbol{x}),(i=1,2,\cdots,K)$ 是每个成员的高斯概率密度函数，则：

$$b_i(\boldsymbol{x})=\frac{1}{(2\pi)^{N/2}\left\|\sum_i\right\|^{1/2}}\exp\{-\frac{1}{2}(\boldsymbol{x}-\boldsymbol{\mu}_i)^{\mathrm{T}}(\sum\nolimits_i)^{-1}(\boldsymbol{x}-\boldsymbol{\mu}_i)\} \tag{11.7}$$

其中，N 为特征向量的维数；$\boldsymbol{\mu}_i$ 和 $\sum_i$ 分别为 $b_i(\boldsymbol{x})$ 的均值向量和协方差矩阵。

对于一个长度为 T 的测试语音时间序列 $\boldsymbol{X}=(x_1,x_2,\cdots,x_T)$，它的GMM似然概率可表示为：

$$P(\boldsymbol{X}\mid\lambda_i)=\prod_{t=1}^{T}p(x_t\mid\lambda_i) \tag{11.8}$$

$$L(\boldsymbol{X}\mid\lambda_i)=\lg[P(\boldsymbol{X}\mid\lambda_i)]=\prod_{t=1}^{T}\lg[p(x_t\mid\lambda_i)] \tag{11.9}$$

识别时运用贝叶斯定理，在 M 个未知话者的模型中得到似然概率最大的模型对应的话者即为识别结果：

$$i^*=\arg\limits_{1\leqslant i\leqslant N}\{\max[L(\boldsymbol{X}\mid\lambda_i)]\} \tag{11.10}$$

在实际应用中，每个 GMM 模型的规模通常取为 30～50 个高斯分布。由于计算 GMM 中的 $p(\boldsymbol{x}\mid M,\theta)$ 需要求解 $N\times N$ 维协方差矩阵 $\sum_i(i=1,2,\cdots,K)$ 的逆，运算量大。为此，常将 $\sum_i$ 设为对角阵，将求逆运算转化为求倒数运算，以提高运算速度。在不匹配条件下，包括电话信道、噪声、信号非线性扭曲等情况，GMM 分类器的性能衰减很厉害，可以通过整合一个针对噪声建立的 GMM 模型来提高系统的鲁棒性。

2．GMM 超向量及其在说话人识别中的应用

GMM 超向量[14]是在高斯混合通用背景模型的基础之上，对话者高斯模型的均值向量运用 MAP 自适应处理得到的。采用 GMM 超向量可以得到几种不同的核函数，应用到 SVM 说话人识别系统[15]中。这是说话人识别系统中核函数选择的一种新尝试。

1）超向量的生成

在传统的高斯混合模型说话人识别系统中，由于话者训练语音有限，当人数较多时，识别性能不佳。而通用背景模型（UBM）利用话者无关的特征分布来近似话者训练语音未覆盖到的发音情况，能很好地弥补话者训练语音不足的缺点，提高系统识别率。与每个话者的高斯混合模型不同的是，UBM 是由所有话者的语音训练得到的，并不是某个特定话者的模型。为了保证训练数据中各种数据的均衡，如男、女语音均衡，可使用训练数据集中的一个子集训练一个小的 UBM，如一个男声模型、一个女声模型，再把这些小 UBM 结合到一起，如图 11.2 所示。这样有利于精确控制背景模型的特性。由于各子集的混合系数相对较小，因此在

使用 EM 算法训练时，计算量小，训练速度较快且可以免受训练数据分布不均的影响。

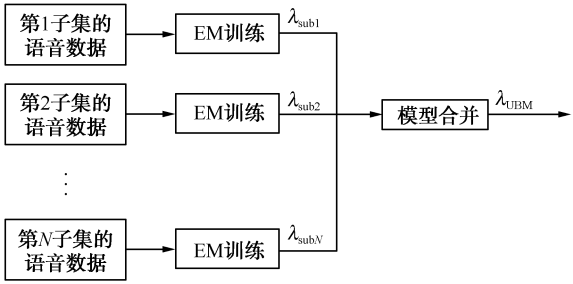


图 11.2　通用背景模型的生成

假设得到的高斯通用背景模型（UBM）为：

$$g(\boldsymbol{x})=\sum_{i=1}^{N}a_i N(\boldsymbol{x};\boldsymbol{m}_i,\sum\nolimits_i) \tag{11.11}$$

其中，a_i 为混合权重，$N()$为高斯密度函数，$\boldsymbol{m}_i$ 和 $\sum_i$ 分别是均值和对角协方差矩阵。

给定一个说话人语音序列 $\boldsymbol{x}=(\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots\boldsymbol{x}_T)$，$\boldsymbol{x}_i\in\mathbf{R}^n$，UBM 使用 MAP 算法对均值 m_i 进行自适应训练，最后得到超向量。其形成过程如图 11.3 所示。

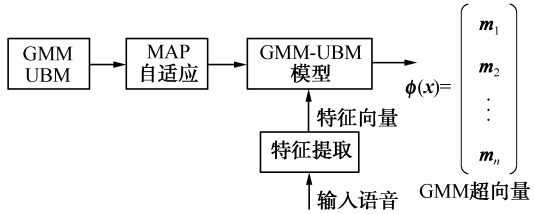


图 11.3　超向量的形成过程

从图 11.3 中可看出，GMM 超向量可以看成是由输入语音序列通过 MAP 映射后得到的高维特征向量，类似于支持向量机的序列核函数的思想。

2）基于 GMM 超向量的核函数

GMM 超向量不仅是定长的，同时对其应用不同的变换方法可得到不同的核函数。

（1）KL 散度线性核函数。

假定两类待识别的语音序列 utt_a 和 utt_b，通过 GMM-UBM 分别得到两类语音的高斯混合模型 g_a 和 g_b。两类语音序列的原始 KL 散度距离为[16,17]：

$$D(g_a \| g_b) = \int_{\mathbf{R}^n} g_a(\boldsymbol{x}) \log_2 \left(\frac{g_a(\boldsymbol{x})}{g_b(\boldsymbol{x})} \right) \mathrm{d}\boldsymbol{x} \tag{11.12}$$

但由于 KL 散度距离不满足 Mercer 条件，直接用于 SVM 非常困难，故用下式近似替代：

$$D(g_a \| g_b) \leqslant \sum_{i=1}^{N} a_i D(N(\boldsymbol{x}; \boldsymbol{m}_i^a, \sum\nolimits_i^a) \| N(\boldsymbol{x}; \boldsymbol{m}_i^b, \sum\nolimits_i^b)) \tag{11.13}$$

其中，m_i^a 和 m_i^b 表示第 i 个单个高斯分布的自适应的超向量。假设协方差矩阵为对角矩阵，这样，式（11.13）可表示为：

$$D^2(\boldsymbol{m}^a, \boldsymbol{m}^b) = \frac{1}{2} \sum_{i=1}^{N} a_i (\boldsymbol{m}_i^a - \boldsymbol{m}_i^b)^{\mathrm{T}} \sum\nolimits_i^{-1} (\boldsymbol{m}_i^a - \boldsymbol{m}_i^b) \tag{11.14}$$

得到不等式：

$$0 \leqslant D(g_a \| g_b) \leqslant D^2(\boldsymbol{m}^a, \boldsymbol{m}^b)$$

GMM 超向量 $\boldsymbol{m}_i^a$ 和 $\boldsymbol{m}_i^b$ 之间的距离 $D^2()$ 表示两个混合模型之间的 Euclidean 距离，这是 KL 散度距离的上限。因此，如果 $\boldsymbol{m}_i^a$ 与 $\boldsymbol{m}_i^b$ 的距离小，相应的 KL 散度就小。

KL 散度线性核函数最早由 Campbell 提出，其核心思想就是从上式中定义的距离 $D^2(\boldsymbol{m}^a, \boldsymbol{m}^b)$ 中寻找内积的对偶表达式。

$$\begin{aligned} K_{\text{linear}}(\text{utt}_a, \text{utt}_b) &= \boldsymbol{\phi}(\text{utt}_a) \bullet \boldsymbol{\phi}(\text{utt}_b) = \sum_{i=1}^{N} a_i (\boldsymbol{m}_i^a)^{\mathrm{T}} \sum\nolimits_i^{-1} \boldsymbol{m}_i^b \\ &= \sum_{i=1}^{N} (\sqrt{a_i} \sum\nolimits_i^{-\frac{1}{2}} \boldsymbol{m}_i^a)^t (\sqrt{a_i} \sum\nolimits_i^{-\frac{1}{2}} \boldsymbol{m}_i^b) \end{aligned} \tag{11.15}$$

特征空间表示为一个与 GMM 超向量空间成一定比例的简单对角矩阵，此式满足 Mercer 条件，可将其直接应用于 SVM。由此可见，utt_a 到 $\boldsymbol{\phi}(\text{utt}_a)$ 的映射实际上就是 $\boldsymbol{\phi}(\text{utt}_a) = \sqrt{a_i} \sum_i^{-\frac{1}{2}} \boldsymbol{m}_i^a$。至此支持向量机的判决函数可表示为：

$$f(\boldsymbol{x}) = (\sum_{i=1}^{L} \alpha_i t_i \boldsymbol{\phi}(\boldsymbol{x}_i))^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}) + d = \boldsymbol{w}^{\mathrm{T}} \boldsymbol{\phi}(\boldsymbol{x}) + d \tag{11.16}$$

这就意味着我们只需要通过计算目标模型和 GMM 超向量之间的内积进行判断。

（2）KL 散度非线性核函数。

KL 散度非线性核函数的方法如下：

$$K_{\text{nonlinear}}(\text{utt}_a, \text{utt}_b) = \mathrm{e}^{-D^2(\boldsymbol{m}^a, \boldsymbol{m}^b)} \tag{11.17}$$

Dehak 和 Chollet 等人首次提出这种非线性核函数。非线性核函数与线性核函数的不同在于特征空间提取的距离不同。非线性核函数是线性核函数的指数化的形式。如前所述，线性

核函数从特征空间提取的是 Euclidean 距离，而非线性核函数的距离表示为：

$$K(\boldsymbol{\phi}(\text{utt}_a),\boldsymbol{\phi}(\text{utt}_b))=\sqrt{2-2\text{e}^{-D^2(\boldsymbol{m}^a,\boldsymbol{m}^b)}} \tag{11.18}$$

在使用该核函数之前，需要将超向量由线性向非线性进行映射 $\boldsymbol{m}\mapsto\boldsymbol{\phi}(\boldsymbol{m})=\text{e}^{-\frac{\|\boldsymbol{m}\|}{2\sigma^2}}$。

（3）L2 内积核函数。

另外一种基于 GMM 超向量的核函数就是 L2 内积核函数。假定两个 GMM 模型 g_a 和 g_b，模型由两输入语音 utt_a 和 utt_b 通过 MAP 自适应获得。一个函数空间的标准内积如下式所示：

$$K(\text{utt}_a,\text{utt}_b)=\int_{\mathbf{R}^n} g_a(\boldsymbol{x})g_b(\boldsymbol{x})\text{d}\boldsymbol{x} \tag{11.19}$$

将 $g(\boldsymbol{x})=\sum_{i=1}^{N}a_iN(\boldsymbol{x};\boldsymbol{m}_i,\sum_i)$ 代入式（11.19）可得：

$$K(\text{utt}_a,\text{utt}_b)=\sum_{i=1}^{N}\sum_{j=1}^{N}a_ia_j\int_{\mathbf{R}^n}N(\boldsymbol{x};\boldsymbol{m}_i^a,\sum\nolimits_i))\times N(\boldsymbol{x};\boldsymbol{m}_j^b,\sum\nolimits_j))\text{d}\boldsymbol{x}$$

$$=\sum_{i=1}^{N}\sum_{j=1}^{N}a_ia_jN(\boldsymbol{m}_i^a-\boldsymbol{m}_j^b;0,\sum\nolimits_i+\sum\nolimits_j) \tag{11.20}$$

其中，0 表示零向量。为了便于计算，假设不同的单高斯模型成分的均值距离很远，即 $\boldsymbol{m}_i^a-\boldsymbol{m}_j^b$ 的值很大，这样 $i\neq j$ 的成分就可忽略了，式（11.20）的核函数可简化为：

$$\tilde{K}(\text{utt}_a,\text{utt}_b)=\sum_{i=1}^{N}a_i^2N(\boldsymbol{m}_i^a-\boldsymbol{m}_i^b;0,2\sum\nolimits_i) \tag{11.21}$$

由超向量得到的以上3种核函数各有优缺点，可以有效地应用到SVM说话人识别系统中。

11.3.4　多类分类支持向量机

如第 4 章所描述的一样，SVM 基于结构风险最小化（SRM）原理，而不是传统统计学的经验风险最小化（ERM）原理，在理论上具有突出的优势，贝尔实验室率先对美国邮政手写数字库识别研究方面应用了 SVM 方法，并取得了较大的成功。在随后的近几年内，有关 SVM 在模式识别领域取得了重大的研究成果，从最初的简单模式输入的直接的 SVM 方法研究，进入到多种方法取长补短的联合应用研究，对 SVM 方法也有了很多改进[18]。

一般情况下，SVM 只能辨别两类数据，需要正反两类数据进行训练，而在实际中多存在多类分类问题。因此，要在实际中应用需要解决多类分类问题，常将两类 SVM 扩展到多类别

分类器。主要方法如下。

1．一对多组合方式分类（one-against-rest）

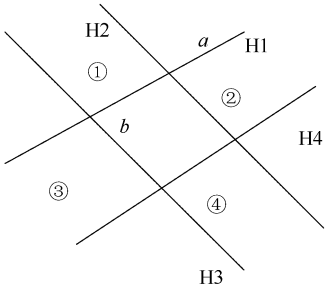


图 11.4　一对多方法

一对多方法如图 11.4 所示，图中的四个圆圈代表四个类，每一条直线都代表一个超平面。从图中可以看出每一个类同其他所有的类都存在一个超平面，这种方法对于 K 类问题需要 K 个 SVM。对于第 K 个 SVM，我们可以得到一个判别函数 $f^k(x)$，最终的分类输出有两种形式。

第一种为：$\Phi(x)=k$，$\mathrm{sgn}[f^k(x)]=1$。

第二种为：取判别函数的输出为最大 SVM，即 $\Phi(x)=\arg\max[f^k(x)]$。

一对多形式构成的多类分类器的分类性能分析如下。

对于这种判别分类方式，由图 11.4 中可以看到样本 a 同时处于超平面 H1，H2 的正侧，按照分类决策准则这时无法判断样本 a 属于第一类还是第二类。再看样本 b 所处的位置，样本 b 位于所有的超平面的负侧，这时无法对 b 进行分类。对于第二种分类的决策方式，当 a 位于图中的位置时可以被分类，但是这时能否被正确分类值得怀疑，即若 a 属于第一类，但离超平面 H1 的距离大于离超平面 H2 的距离时，这时决策输出的结果为第二类，为错误的分类结果。对于样本 b，这种分类决策方式同样存在无法分类的情况。由图 11.4 可以看出一对多的方式产生分类错误的根本原因是各个超平面的分类结果存在交叠的区域，例如，当一个属于第一类的样本用第一个超平面分类时显示为第一类，当用第二个超平面分类时如果也输出正值，这时就产生了无法正确分类的情况。实际上，对于属于第一类的样本只有第一个超平面对这个样本分类才有意义，而其他的超平面的分类结果可以看做是分类噪声，但是我们无法在分类之前就知道该样本到底属于哪一类，所以在分类判别中只好对各个超平面的分类结果平等对待，这样也就无法去除或抑制分类噪声，所以不能得到满意的分类结果。

2．一对一组合方式分类（one-against-one）

在这种方法中，需要对每两个不同的类的样本训练一个 SVM 分类器，所以称为一对一的方法[19]，在这种方法中，其组合的方法如图 11.5 所示。图中的例子为一个四个不同类别的多类分类器。图中的四个圆圈代表四个不同的类，图中实线表示超平面，对于虚线两端的两个类进行分类。从图中可以看出在每两个类之间都有一个分类器。

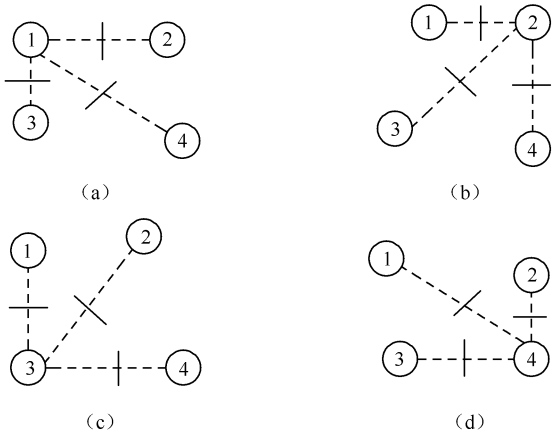


图 11.5　一对一方法中组合的方法

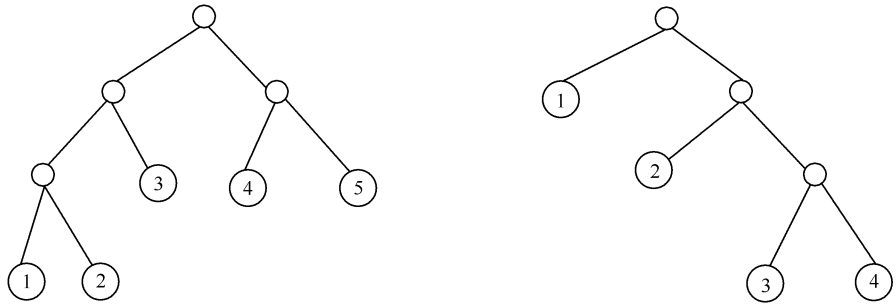
一对一形式构成的多类分类器的分类性能分析如下。

当对一个属于第 K 类的样本进行分类时，当所有的与 K 类有关的分类器的输出都正确时，$f^k = K-1$，显然这种情况下可以正确分类。当与 K 有关的分类器有 a 个发生分类错误时，$f^k(x) = K-1-2a$，由于分类器的分类效率很高，所有 a 通常都很小，此时只有当存在某一个分类器 j 的函数 $f^j(x) > f^i(x)$ 时才能产生错误的分类结果。第 i 类的样本对于第 K 类有关的分类器可以看成是随机的输入，通常第 i 类的样本对于与第 j 类有关的分类器产生的 $f^j(x)$ 都很小，所以要使 $f^j(x) > f^i(x)$，这样的概率是很小的。只有当样本比较接近第 j 类的中心时，与第 j 类有关的分类器往往显示这个样本为第 j 类的样本，这样才导致了最终的分类错误。所以，总体上这种由二类分类器组成的多类分类器的分类效果很好，但是由于需要由 $K(K-1)/2$ 个二类分类器构成，这一点限制了这种分类器的使用。

3．二叉树组合方式分类（H-SVMs）

二叉树组合方式分类是一种多级的结构[20]，即在每一级把问题再划分成两个子问题，这样在其最后的一层就可以完全解决多类的分类问题，这一解决问题的方法就是采用了二叉树的方法。用 SVM 采用二叉树的方法来解决多类的问题通常可以采用两种结构，一种是对称的结构，另外一种是非对称的结构，如图 11.6 所示。图 11.6（a）中是对称的结构，它在每一级中尽量把问题划分成规模相当的两个子问题，这样划分问题的意义是可以用最少的级数来解决问题，从图中可以看到，如果要解决一个 K 类问题需要有$[\log_2 K]$个级划分来解决，共需要 $K-1$ 个 SVM 分类器。图 11.6（b）中的结构为非对称的方式，在它的每一级都可能得到一个最终的分类结果，这种方法同样需要 $K-1$ 个分类器，但是却要有 $K-1$ 级划分。这种结构在扩

展时，只要在最后的一个节点上继续添加分类器就可以了。



（a）对称结构　　（b）非对称结构

图 11.6　二叉树的结构

二叉树方法是一种非常直观的解决问题的方法，它的解决问题的思路是不断地把问题划分成更小的规模的问题来解决。但是采用二叉树方法来构造 SVM 多类分类器不可避免地带来决策树的一些缺点。比如错误是自上向下传播的，也就是前一级产生的错误分类将导致最终的分类错误。所以，在构造二叉树时通常要尽量避免采用太多的级数的划分。再者，每一级划分中的两类的不同组合产生的分类效果是不同的，由于其分类效果的传播性，所以各个分类器要精心地调整其所分的两类的组合方式，在实际运用中这种调整是相当麻烦的。

以上是由二类 SVM 分类器构成多类分类器的常用方法。其中，一对一的方法具有最强的分类能力，能够产生最好的分类效果，但是需要的 SVM 分类器也最多，对于一个 K 类的问题需要 $K(K-1)/2$ 个 SVM。由于这种方法所需要的 SVM 的个数与 K 是成平方的关系增长的，当 K 达到了一定的规模时就需要训练大量的 SVM，这一点限制了这种方法的应用。一对多的方法对于 K 类问题只需要 K 个 SVM，但是由于各个分类器存在交叠的区域，即使所有的分类器都输出正确的分类结果，最终的分类结果也不一定正确，所以这类分类器的分类效果不理想。二叉树的方法是一种通过二类问题解决多类问题的一种最直观的方法，但是由于其误差的自上向下的传播，以及各级的不同的组合方式对最终的分类结果的影响限制了二叉树的构建及最终的分类效果。

11.3.5　人工神经网络法（ANN）

说话人识别包含从低层次到高层次的各个阶段及其彼此之间的相互作用，是一个非常复杂的模式识别问题，模式识别的最新技术——人工神经网络，尤其适合于这类问题。在目前

还没有找到把说话人所说话的内容特征和说话人自身的个性特征如何从说话人所发语音的语音特征中分离出来的办法。人工神经网络已经应用在说话人识别的各个层次，但至今成功的例子多数集中在说话人个性特征提取到说话人识别这一层次上。用于说话人识别的神经网络种类也是多种多样的，但大部分集中在多层感知器结构的神经网络上。从总体上讲，基于神经网络的说话人识别目前还处于研究和实验阶段，对于大规模应用方法的研究刚刚起步，尤其是对于实际的说话人识别系统应如何构成这一问题目前还在进一步研究中。

1．说话人识别的神经网络模型结构

在各种人工神经网络模型中，在说话人识别中应用最多的也是最成功的当数多层前馈网络，其中又以采用 BP 学习算法的多层感知器（BP 网络）为代表。具体做法就是将说话人的个性特征作为网络的输入，通过监督学习方式进行训练，利用神经网络强有力的分类能力，使网络完成说话人个性特征到说话人身份编码的非线性映射。在测试语音的特征参数输入网络时，在网络的输出端得到说话人的身份结果，如图 11.7 所示。

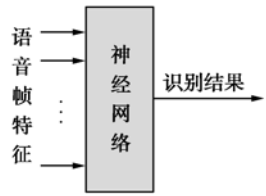


图 11.7　神经网络用于说话人识别的过程

在利用神经网络模型进行说话人识别时，由于网络模型结构一旦确定下来，网络的结构、输入节点数目、输出节点数目、说话人识别系统所需建立的网络的数目就是固定不变的，而这些参数的选取不仅要考虑网络模型的性能，还要考虑网络模型的训练问题。

神经网络用于说话人识别，系统模型有以下三种基本结构。

（1）为所有说话人建立一个神经网络模型，用这一个网络实现对所有人的分类和识别。这样的网络模型有多个输出节点，每一个输出节点对应一个说话人。网络的结构是输入节点数等于语音特征的维数，而输出层的节点数等于说话人的总数。具体做法是，在训练阶段，如果用于训练的输入训练样本对应说话人 i，则训练时网络输出层的第 i 个节点的期望输出是 1，而其余输出节点期望输出为 0。并且对于这个神经网络模型，利用所有说话人的训练样本，对网络进行有监督的训练。在识别阶段，当一个未知说话人的语音特征参数作用于训练好的网络时，考察各输出节点的输出，并将具有最大输出值的节点对应的说话人判定为待识别的人。

（2）为每一个说话人建立一个神经网络，用这一网络实现该说话人与其他说话人的分类和识别。这样的网络模型只有一个输出节点，而输入层节点数依然等于语音特征参数的维数。具体做法是，为每个说话人建立这样一个网络，对每个网络进行分别训练，当对应网络的说话人的训练样本输入时，期望输出为 1，而当其余说话人的训练样本输入时，期望输出为 0。在识别阶段，将一个未知说话人的语音特征参数作用于训练好的每个神经网络，考察各个网

络输出节点的输出，并将具有最大输出值的网络对应的说话人判定为待识别的人。

（3）为每一对说话人建立一个神经网络，用这一网络实现这一对说话人的识别与分类。这样的网络模型只有两个输出节点，分别对应于所区别的这两名说话人，而输入层节点数依然等于语音特征参数的维数。具体做法是，为每对说话人建立这样一个网络，对每个网络进行分别训练，对于每个网络只用对应的这一对说话人的训练样本，当其中一个说话人的训练样本输入时，其中一个输出节点期望输出为 1，而另一个节点期望输出为 0。反之当另一个说话人的训练样本输入时，期望输出正好相反。在识别阶段，识别结果将取决于这些网络组成的神经网络树的识别结果。

和其他模式识别任务一样，在这里建立并且训练的神经网络模型就相当于对说话人建立特征参考模板，在后续的识别阶段，就是用待识别的说话人语音特征来匹配这些模板的过程，最后匹配的结果根据某种阈值算法来决定识别结果。

2．神经网络用于说话人识别所遇到的问题

在应用人工神经网络构建说话人识别系统时，在许多神经网络类型中，前向神经网络以其结构简单、分类性能较好在说话人识别中获得了广泛的使用。多层前向神经网络是映射型神经网络，可完成从说话人特征空间向说话人集合的映射。但是，一个神经网络要具有良好的性能，必须要经过训练来完成，而训练的时长、网络是否收敛是决定这一网络模型可行性的关键，这些问题取决于任务本身的复杂程度。

对于说话人识别这一任务，它的技术难点中包含：特征空间有限性。即对于由某个或某些特征参数构成的有限特征空间，包含 N 个人的识别系统要将其划分为 N 个子空间，当 N 很大时，特征子空间就有可能产生交集，从而降低系统的正确识别率。而在说话人识别中，待识人群往往很大。随着待识别人群数目的增加，说话人特征分布间重叠区域增加，分类器不能将所有说话人的特征在特征空间完全区分开，说话人识别率将降低。换句话说，在识别过程中不可避免地存在着说话人特征参数的有限性与说话人特征空间无穷划分之间的矛盾，这是所有说话人识别方法所面临的共同问题。

在神经网络用于说话人识别中，这一问题又以新的形式显现出来。当待识别人群数目增加时，网络的训练时间急剧增加，理论上当人群数目很大时，将无法完成网络的训练[21]。

如果采用建立一个大网络的方法，用这一个神经网络对所有说话人进行分类和识别，这要求用所有说话人的语音对网络进行训练。训练好的网络的连接权值是所有可识别的说话人的特性的隐含表示，这种形式虽然只需建立一个神经网络，但是网络的规模较大，分类任务复杂，网络不易收敛，权系数要求较多，存储容量较大，训练时间较长。而且一旦网络模型确定下来以后，当要系统识别的说话人增加时，网络结构随之改变，需要重新对网络进行训练，使其扩展性不好，无灵活性，而且训练时间以指数增长,并且性能下降。

如果为每一对说话人建立一个神经网络，则对以 N 个说话人系统来讲，总共需要 $N(N-1)/2$ 个网络，并且每增加一个说话人，必须相应地再训练 N 个网络，网络数目非常大，网络结构复杂。

11.3.6　混合方法

在上述几类说话人识别方法中，模板匹配算法优点在于复杂度低，训练时间短，训练和识别计算量小，但识别率不高；概率统计模型的优势在于能够全面反映说话人语音特征参数的统计特性，识别率高，但复杂度较高，训练时间长，训练和识别计算量大；基于判决的模型具有很强的分类能力，但训练时间长。

由于不同的识别方法各自具有优缺点，因此在说话人识别系统中，经常将两种或两种以上的模型进行混合，取长补短，以改善识别系统的性能。例如，HMM 模型和 DTW 模型、HMM 模型和人工神经网络、HMM 模型和支持向量机、GMM 模型和支持向量机等模型的混合，但混合模型的复杂度高，计算量加大。同时，在特征参数的提取方面，也经常采用将语音特征参数进行混合的方法。

11.4　说话人识别的系统性能评价标准

一个说话人识别系统的性能可以从系统的识别结果来评价。对于说话人辨认来说，识别的结果只可能是正确或错误两种，正确识别的概率与错误识别的概率之和为 1。因此，可简单地用正确识别的概率（常称为识别率）或错误识别概率（常称为错误率）作为评价识别系统性能的指标[22]。对于说话人确认系统来说，表征其性能的最重要的两个参量是错误拒绝率（False Rejection Rate，FRR），又称为 I 型误差；以及错误接受率（False Acceptance Rate，FAR），又称为 II 型误差[23]。前者是拒绝目标说话人所造成的误差，后者是将冒名顶替者错认为是目标说话人而引起的误差。

11.4.1　说话人辨认

说话人辨认系统中的错误率 E_{SI} 或正确率 C_{SI} 可以表示为：

$$E_{\mathrm{SI}} = n_{\mathrm{error}} / n_{\mathrm{test}} \tag{11.22}$$

$$C_{\mathrm{SI}} = n_{\mathrm{correct}} / n_{\mathrm{test}} \tag{11.23}$$

在上面两式中 n_{error}，n_{correct}，n_{test} 分别表示错误数、正确数和总测试数。

11.4.2 说话人确认

在说话人确认系统中，错误拒绝率 FRR 和错误接受率 FAR 通过下面的公式计算：

$$\mathrm{FRR} = n_{\mathrm{FRR}} / n_{\mathrm{target}} \tag{11.24}$$

其中，n_{target} 和 n_{FRR} 分别表示目标话者的测试数和目标话者未被测试出的实验次数。

$$\mathrm{FAR} = n_{\mathrm{FAR}} / n_{\mathrm{imposter}} \tag{11.25}$$

其中，n_{imposter} 和 n_{FAR} 分别表示冒名顶替者的测试数和目标话者被错误测试出的次数。

通常将错误拒绝率和错误接受率结合起来，寻找二者相等的点得到等错误率（Equal Error Rate，EER），用于衡量说话人确认系统的性能。

在说话人识别系统中，除了以上几种系统性能评价指标外，还要注意以下几个方面。

1）系统的鲁棒性

说话人识别系统由一定条件下所采集的大量语料训练而成，采样的环境可能受到背景噪声、信道失真、说话人语调及情绪等的影响，使得系统的性能急剧下降。因此，在说话人识别系统中必须考虑到系统的鲁棒性，寻找具有鲁棒性的参数，要求其具有以下条件：

（1）能有效区分不同的说话人，含有说话人的个性特征；

（2）对同一说话人，当说话人的说话方式改变时特征参数变化小；

（3）抗噪声和信道干扰能力强。

2）复杂度

复杂度是说话人识别系统能否实现的关键因素。通常说话人系统的复杂度是指模型的复杂度和计算复杂度。模型复杂度的降低，即可降低算法的存储空间，又可减少计算量，便于算法的实现。计算复杂度直接关系到说话人识别系统的实时性。

11.5 改进的说话人识别算法及系统

11.5.1 支持向量机在说话人识别中的应用改进实例

起初 SVM 在说话人识别中的应用主要是与 HMM 模型、GMM 模型融合使用，充分利用了支持向量机的基于结构风险的分类能力，取得了很好分类的效果。参考文献[24]直接构建了基于 SVM 的说话人识别系统，用全部的语音特征参数训练 SVM，在不考虑时间的情况下，取得了很好的整体效果。

为了减少标准 SVM 算法的计算量，Lee 和 Msngasarian 在 2001 年提出了约简支持向量机（Reduced Support Vector Machines，RSVM）[25]，基本思想是从训练样本集里面随机选取一些样本作为“支持向量”，用这些少量的支持向量代替整个训练数据训练 SVM，大大减少了 SVM 的计算量，但是，在此方法中，“支持向量”是任意选取的，没有代表性，因而系统不够稳定。此后有好多学者对其进行了改进，如参考文献[26]提出用无监督聚类的聚类中心作为支持向量，参考文献[27]提出密度聚类的选择支持向量方法，2004 年 SUN 等人[28]将约简支持向量机（RSVM）算法应用在说话人识别中，对说话人的语音特征参数用 *K*-均值聚类，并选择离质心较远的样本作为支持向量，在没有使识别率降低太多的情况下，减少了 SVM 的训练量。但是在说话人识别中，提取的语音特征参数在数据空间具有一定的重叠，且是线性不可分的。为克服上面的不足，提出了一种多约简方法（如图 11.8 所示），语音特征参数用 PCA 变换降维、去噪，减少存储空间，增强系统的鲁棒性，再利用核聚类对于线性不可分和不对称样本具有很好的聚类能力的优点，对语音特征参数进行模糊核聚类，根据样本选择算法约简语音特征参数样本，从而减少了系统的存储空间和 SVM 的训练量，增强了系统的鲁棒性。

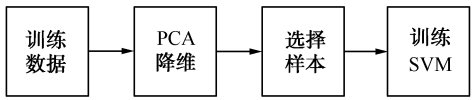


图 11.8　一种多约简方法

1．PCA 降维

假设有 n 个注册的说话人，每一个说话人的训练语音信号由 M 段语音 $(S_1^s, S_2^s, \cdots, S_M^s)$ 组成，包含了说话人 s 的不同发音及语音韵律等特征。对其进行去噪、去静音，合成一个完全由语音数据组成的语音信号 $S^s(n)$，对 $S^s(n)$ 分帧、加窗、提取 12 维 MFCC 倒谱系数及其一阶差分，得到 N 个 24 维的语音特征矢量序列 $(\boldsymbol{m}(i), i=1,2,\cdots,N, \boldsymbol{m}(i)\in\mathbf{R}^{24})$。将其表示成一个 $N\times 24$ 维的矩阵，PCA 降维算法如下。

Step 1：求出语音特征矢量的均值向量，$\boldsymbol{\mu}_j=\dfrac{1}{N}\sum_{i=1}^{N}\boldsymbol{m}_j(i),\ j=1,2,\cdots,24$。

Step 2：计算中心化的语音特征矢量，$\boldsymbol{m}'(i)=\boldsymbol{m}(i)-\boldsymbol{u}$。

Step 3：计算协方差矩阵，$\boldsymbol{S}=\dfrac{1}{n-1}(\boldsymbol{m}(i)-\boldsymbol{u})^{\mathrm{T}}(\boldsymbol{m}(i)-\boldsymbol{u})=\dfrac{1}{n-1}\boldsymbol{m}'^{T}(i)\boldsymbol{m}'(i)$。

Step 4：计算协方差矩阵的特征值和其对应的特征向量，即$\lambda_1\geqslant\lambda_2\geqslant\cdots\geqslant\lambda_{24}$对应的特征矢量为 $\boldsymbol{w}_1,\boldsymbol{w}_2,\cdots,\boldsymbol{w}_{24}$，取前 14 个特征值和特征矢量，由 PCA 变换定义得 $\boldsymbol{Y}(i)=\boldsymbol{W}^{\mathrm{T}}\boldsymbol{X}'(i)$。

Step 5：重构语音特征矢量，$\hat{\boldsymbol{X}}'=\boldsymbol{W}\boldsymbol{Y}(i)$。

在 PCA 降维中，由于只采用了前 14 个最大的特征值及对应的特征向量重构特征矢量，所以维数从 24 维降到了 14 维，存储量大大减少。且经过降维后，重构的语音特征矢量也滤除了一部分噪声。

2．选择样本

为任意两个注册说话人建立一个 SVM，其模型如图 11.9 所示，圆和三角符号分别代表两个说话人的语音特征矢量。若采用 15s 的录音，大致有 1000 个语音特征矢量，标准的支持向量机训练方法是把这些语音参数全部作为支持向量，其训练量非常大。为减少训练量，本文对语音参数样本进行约简，只选择对分类有意义的语音参数。即对语音参数模糊核聚类，采用同一个径向基函数训练 SVM，使得聚类结果和 SVM 在同一高维空间。由上述 SVM 的原理可知，SVM 的最优超平面由少数支持向量决定，且不可能通过聚类的中心，所以聚类中心的语音参数对分类并没有太大的影响，仅仅增加了训练量。选择每个聚类的边界样本作为支持向量，训练 SVM，在不影响分类效果的情况下，大大减少了训练量。

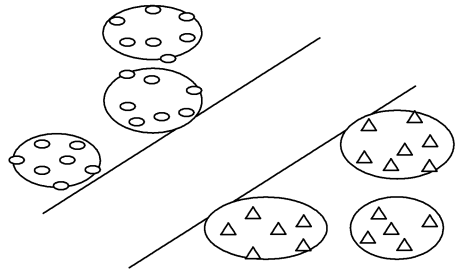


图 11.9　一个 SVM 模型

在核空间完成样本选择，对任意一个注册说话人来说，选择的样本放入集合 $M^s, s=1,2,\cdots,n$，n 为注册说话人的人数。

具体步骤如下。

Step 1：初始化 $M^s=0$，s=1。

Step 2：计算每一聚类的门限 T_j。

① 对 $m_i^j \in V_j^s, j=1,2,\cdots,C$，$C$ 为聚类数，计算到聚类中心 v_j^s 的距离 $d_F^2(m_i^j, v_j^s)$，采用径向基核函数（RBF）作为核函数，则 $d_F^2(m_i^j, v_j^s)=2-2K(m_i^j, v_j^s)$。

② 找出样本到聚类中心的最大距离 $D_j=\max\limits_i(d_F^2(m_i^j, v_j^s))$。

③ 计算聚类 V_j^s 的门限 T_j，$T_j=\alpha_j D_j$。$\alpha_j \in (0,1)$ 为调节因子。

Step 3：若 $d_F^2(m_i^j, v_j^s)>T_j$，m_i^j 加入 M^s 集中，否则丢弃该语音参数。

Step 4：若 $s=n$，结束选择，否则重复 Step 2、Step 3。

根据此算法选择样本，其中 α_j 为调节因子，调节 α_j 的值，可以得到不同程度的约简。α_j 越大，约简的语音参数越多，若采用 $\alpha_j=1/2$，大致可以将样本约简到原来的 1/2，则训练量减少了一半。

3．多级辨识方法

说话人辨识就是判定待测说话人的语音属于多个参考说话人之中的某一个，每一次辨识需要将待测语音去匹配所有说话人的参考模型，找出最相近模型所对应的说话人作为辨识结果，这样必然导致注册人数越多，花费时间越长，当注册人数达到一定数量后，系统很难满足实时响应。对此一些学者提出了自己的解决方案，如 Bing Sun 等人[29]提出用说话人 GMM 模型之间的模型距离定义类模型，识别时先进行类模型识别，然后在对应的类模型中寻找目标说话人。We-HoTsai 等人[30]提出用 GMM 模型的 KL 距离，把相似的说话人聚在一起。侯风雷等人[24]根据 GMM 模型的距离定义相似度，将声音类似的说话人聚集为同一类。这些方法的共同特点是利用 GMM 模型定义距离，其缺点是首先要训练每个说话人的 GMM 模型，且 GMM 模型是一种概率统计模型，随着注册说话人数的增多，提取的语音特征矢量之间重叠较为严重，用 GMM 模型进行识别时，识别率下降很快。而 PCA 分类器不需要训练，直接可由语音特征矢量求得，实现比较快速、简单，且 SVM 是一种基于结构风险最小化原则的模式分类方法，在处理样本中非线性、高维数问题时有很大的优势，应用基于语音特征样本的说话人识别上有良好的效果，不会随着注册说话人数的增多而使识别率下降。所以利用 PCA 分类器和 SVM 的各自优点，建立多级说话人辨识系统[20]。

SVM 是一种两元分类器，在构成的多元分类器中，常用一对多组合分类和一对一组合分类。在一对多组合分类中，每当候选集中加入一个新的说话人时，系统都需要重新训练，系统可扩性不好；一对一组合分类虽然只需要加入新的说话人的模板，但是未知说话人的语音要通过多个 SVM 的分类才能得到最后的结果，识别速度太慢。这里用多级说话人辨识方法有效地解决了这个问题。例如，有 n 个注册说话人，首先建立 $n\times(n-1)/2$ 个一对一的说话人模型 MRSVM。在识别阶段，根据正确 PCA 的分类原则（在正确子空间的投影应该比在别的子空间上的投影方差大），用 PCA 分类器对待测语音进行粗分类，取方差最大的前 M 个说话人作为可能的目标说话人。然后从训练好的 MRSVM 数据库中，提取此 M 个说话人构建的 $M\times(M-1)/2$ 个 MRSVM 模型，在这些模型中做出最终的判决。传统的识别方法是将待测语音输入到所有的 MRSVM 模型中，需要判决 $n\times(n-1)/2$ 个 MRSVM 模型，而上面根据预判决只需判决 $M\times(M-1)/2$ 个 MRSVM 模型，大大减少了预判决的 MRSVM 模型个数，从而大大提高了辨识速度。当系统增加一个新的说话人时，只需增加此说话人和原来注册说话人之间的 MRSVM 模型即可，不需训练整个系统。当撤销说话人时，直接撤销此说话人的相关模型，

其余模型不变，所以系统可扩性比较好。整个系统流程如图 11.10、图 11.11 所示。

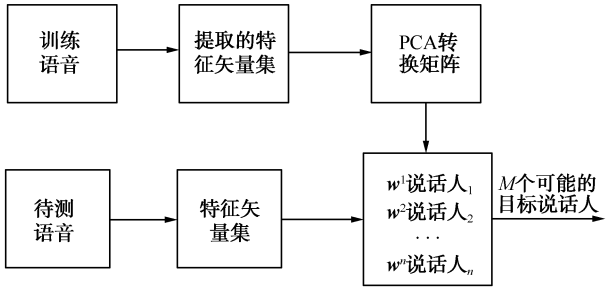


图 11.10　PCA 一级判决的系统流程

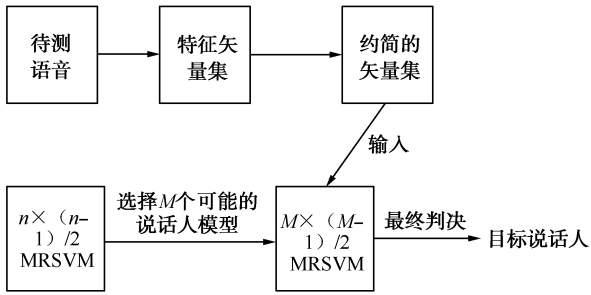


图 11.11　MRSVM 终判决的系统流程

PCA 粗分类：对每一个注册的说话人来说，在上述的 PCA 一级判决中，得到了 PCA 的 $\boldsymbol{W}^s, s=1,2,\cdots,n$，$n$ 为注册的说话人人数，在此主成分子空间中，使得原矢量向其投影后保留的方差总和最大，保留的方差总和为 $\lambda=\sum_{i=1}^{14}\lambda_i$。即：

$$\lambda=\mathrm{Var}(\boldsymbol{y}_1)+\mathrm{Var}(\boldsymbol{y}_2)+\cdots+\mathrm{Var}(\boldsymbol{y}_{14})=(\boldsymbol{w}_1^{\mathrm{T}}\boldsymbol{x})^2+(\boldsymbol{w}_2^{\mathrm{T}}\boldsymbol{x})^2+\cdots+(\boldsymbol{w}_{14}^{\mathrm{T}}\boldsymbol{x})^2=(\boldsymbol{W}^{\mathrm{T}}\boldsymbol{x})^2$$

对于一段待判决的语音信号，用 PCA 作为粗分类，首先对其预处理，并提取特征矢量 $\boldsymbol{X}$，计算在子空间的投影方差：$\lambda^s=\left\|\boldsymbol{W}^{s\mathrm{T}}(\boldsymbol{X}-\boldsymbol{m}_s)\right\|^2$，根据 PCA 的分类依据，$\boldsymbol{X}$ 在正确子空间的投影应该比在别的子空间上的投影方差大，为了减小识别误差，我们可以取方差最大的前 M 个说话人作为预选的目标说话人。

MRSVM 终判决：根据预判决的结果，从训练好的 MRSVM 库中，提取此 M 个说话人之间的 MRSVM 模型，再用待测语音的特征参数作为 MRSVM 的输入，用投票法做出最终的判决。

11.5.2　基于组合神经网络的说话人识别系统

1．系统模型的构建

在 11.3.5 节中我们提到了，为了实现 N 个说话人的识别，通过建立和训练一个规模较大的 BP 网络区分和识别说话人的方法，若要求系统能识别的说话人数目 N 较大，就需构建较大规模的网络，使得网络的隐含层节点数较多，需要的存储量较大。一旦能识别的说话人数目确定，就可以将所需建立的多层感知器网络的规模确定下来，并训练网络，使网络具有说话人识别能力。但是若要对说话人特征库的模板进行修改，或要增加一个模板等，则必须用所有说话人语音对网络进行重新训练，这相当于推翻原来已建立的说话人模板库，重新建立新的说话人模板库，而多层感知器的一个非常大的缺点是训练速度相当慢，当网络规模较大时尤其如此，给系统的扩充、修改和维护带来很大的不便，尤其是在较大量地增加系统能识别的说话人数目时，可能系统的隐节点数目也需要增加，所以用单一的多层感知器网络进行说话人识别在系统结果和性能上都是不理想的。

因此，在使用神经网络进行说话人识别时，更加迫切地需要解决大人群识别问题，解决大人群分类问题的一种方法是先将大人群划分为很小的小人群，再在小人群间进行组合以完成大人群分类问题。

我们下面将对说话人系统进行模块化设计，通过构建多个规模较小的神经网络以模块化、积木化的结构实现说话人识别系统，每一块积木都是结构相同、规模却较小的神经网络。因此，提出一种组合神经网络，为每一个人建立一个子网，每个子网只需识别本人与其他人两种模式，即只需完成二元分类。这样子网结构简单，分类性能好，收敛速度快。N 个子网构成一个用于 N 个说话人识别的大网络。

具体做法是，对每个说话人均建立一个神经网络模型，网络输入层节点数目为特征参数的维数，即 12，网络输出层只有一个节点，用来识别本人与其他人。每个子网的训练样本由本人的样本与其他人的样本组成，每一个子网必须进行有监督的训练，本人训练样本输入时，目标输出为 1，其他人训练样本输入时，目标输出为 0。由于每个网络只是完成一个二元分类的任务，则子网不论是在规模还是结构上都非常简单，在训练时，子网能够快速地收敛到理想的状态，训练时间较短。在识别阶段将待识别语音特征输入到每一个子网，如果某个子网的输出接近于 1（或大于某个阈值），则判断该说话人为这一子网对应的说话人，如果有多个子网的输出均大于阈值，则将具有最大输出的子网对应的说话人判定为待识别的人。

N 个子网构成一个用于 N 个说话人识别的组合型神经网络。每个子网的训练既快速又独立。并且，当 N 只少量增加时，已建立的子网无须重新进行训练，只需为新加入的说话人训

练其对应的子网，系统模型具有较好的扩展性。

构建的基于组合神经网络的说话人识别系统结构模型如图 11.12 所示。

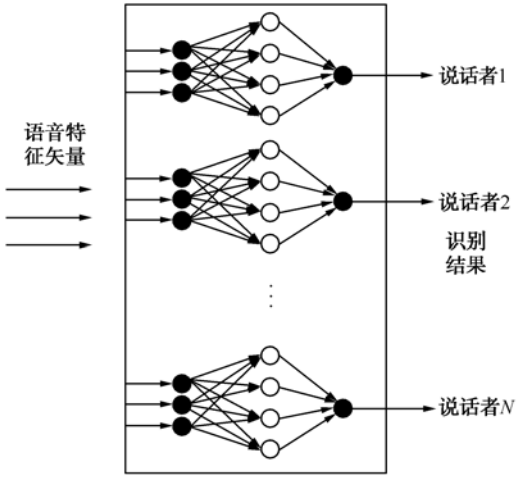


图 11.12　基于组合神经网络的说话人识别系统结构模型

2．神经网络的选取

目前，文本无关的说话人识别广泛使用的是基于非参数模型的 VQ 模型和基于参数模型的 GMM 模型。VQ 模型的基本思想是为每个说话人建立一个码本，它是由语音特征空间中的少数具有代表性的矢量中心构成的，这些矢量中心是通过聚类算法得到的。在识别阶段根据某种相似性测度找出与待识别语音特征最近的码本。GMM 模型是把说话人的语音特征用一个在特征空间分布的概率密度函数来描述，而这一特征分布用高斯分布的加权和来逼近。

鉴于上述两种说话人识别方法的核心思想，选用聚类功能较好的神经网络——RBF 网络。它的隐含层节点代表了特征空间的聚类中心，我们可以借鉴 VQ 模型的方法，利用某种聚类算法来选取隐含层节点，并选取隐含层的基函数为高斯函数，则输出层可完成高斯函数的加权和，这与 GMM 模型有着相似之处。这样隐含层节点已大致描述了说话人特征在特征空间的分布情况，网络收敛速度将明显提高。

RBF 是一种单隐含层的两层前向网络，其输出是隐含层基函数的线性组合，隐含层基函数一般选高斯函数，该基函数能对输入产生局部响应，从而将输入空间划分成若干小的局部区间，以达到分类和函数逼近的目的。隐含层高斯函数的表达式为：

$$\Phi_j(\boldsymbol{x}) = \exp\left\{-\frac{1}{2}(\boldsymbol{x}-\boldsymbol{t}_j)^{\mathrm{T}}\sum\nolimits_j{}^{-1}(\boldsymbol{x}-\boldsymbol{t}_j)\right\}, j = 1, 2, \cdots, N_c \tag{11.26}$$

式中，$\boldsymbol{t}_j$ 为隐含层第 j 个中心节点；$\sum_j = \sigma_j \boldsymbol{I}$，$\sigma_j$ 为该中心的方差；$\boldsymbol{x}$ 为输入特征矢量；$\Phi_j(\boldsymbol{x})$ 为该隐节点输出，在 0～1 范围内。当输入越靠近高斯分布的中心时，隐节点输出越大，RBF 输出层节点完成隐含层输出的线性组合：

$$y_i = \sum_{j=1}^{N_c} \omega_{ij}\Phi_j(\boldsymbol{x}) \tag{11.27}$$

y_i 为输出层第 i 个节点的输出，ω_{ij} 为连接该节点与隐含层节点 j 的权值。故而 RBF 实现了高斯函数的加权和。

当用 RBF 网络来解决一个复杂的模式分类时，它潜在的合理性来自模式可分的 Cover 定理：在低维空间（输入层）非线性可分的问题可映射到一个高维空间（隐含层），使其在高维空间线性可分。

理论上可以证明：RBF 能够像 BP 网络一样逼近任何一个非线性函数，但是与 BP 网络不同的是，RBF 网络的训练速度通常比 BP 网络快得多。这是因为 RBF 是采用局部调节的方法来实现对函数的逼近的，一旦隐含层参数确定下来后，输出层的连接权值就很容易计算。对于说话人识别这一高度非线性映射的任务，选取具有收敛速度快，训练时间短的 RBF 对于提高系统的性能是非常重要的。

11.5.3　基于 TES-PCA 分类器和 KFD 的多级说话人确认

线性判别分析（Linear Discriminant Analysis，LDA）也称为费歇判别分析（Fisher Linear Discriminant，FLD）。1936 年，Fisher 在他的经典论文中第一次提出了表示不同特征变量的线性判别函数，1970 年 Foley 对 Fisher 线性判别技术进行了深入研究，并将其应用于解决两类数据分类问题中。FLD 的判别依据是 Fisher 准则，基本思想是在最大化样本的类间离散度的同时最小化样本的类内离散度，从而确定原始向量的投影方向，使各类之间最大程度地分离，从而达到正确的分类。在说话人识别中，处理的对象为语音数据，它的分布呈非线性，FLD 显得过于简单，并不能达到很好的分类效果。S. Mika 等人[31]对 FLD 进行了非线性的扩展，提出了基于核函数的 Fisher 判别（Kernel Fisher Discriminant，KFD）方法，它将非线性的输入空间通过核函数映射到高维空间，在此高维空间使用 FLD 进行分类。同时，S. Mika 指出由于 KFD 使用了所有的训练样本，而不是少量的称之为“支持向量”的样本，因此 KFD 在某种程度上，分类性能优于支持向量机（Support Vector Machine，SVM）。但是 KFD 所需要

的时间和内存开销与输入样本的数目密切相关，随着样本数目的增加，KFD 的求解难度急剧提高，并有可能导致相关计算无法进行[32]。

主成分分析（Principal Component Analysis, PCA）是一种经典的统计方法，它对多元统计观测数据的协方差结构进行分析，以期求出能简约地表达这些数据依赖关系的主分量。在参考文献[33]中，使用 PCA 对特征向量进行降维，实验结果显示 PCA 可以有效地去除特征向量中的冗余，从而降低向量的维数。PCA 变换不仅具有出色的降维性能, 它还可以进行数据的快速分类。由 PCA 的变换矩阵可以得到两个扩展子空间：主成分空间（Principal Component Space，PCS）和截断误差空间（Truncation Error Space，TES）[34]。主成分空间由主分量构成，而截断误差空间由未选择为主分量的剩余分量构成。按照 PCA 的定义，在 PCS 和 TES 两个空间上可以构造不同的分类器。PCA 分类器具有分类速度快，建模容易，计算简单的优点。

基于此，下面首先构建了一个基于 TES 的 PCA 分类器进行特征向量的降维和注册说话人的初次筛选，然后采用 KFD 进行最终的确认。

1．TES-PCA 分类器

在说话人确认系统中，说话人的语音样本规模较大，直接使用 KFD 进行分类识别，求解的计算复杂度较高，甚至相关计算有可能无法进行。基于此，本文提出一种多级说话人确认方法，系统框图如图 11.13 所示。在该方法中，说话人的确认分为两个阶段：第一阶段是采用 TES-PCA 对注册的 N 个说话人特征向量降维的同时，初次筛选出可能的 R 位说话人；第二阶段就是采用 KFD 在这 R 位说话人中找出最终结果。

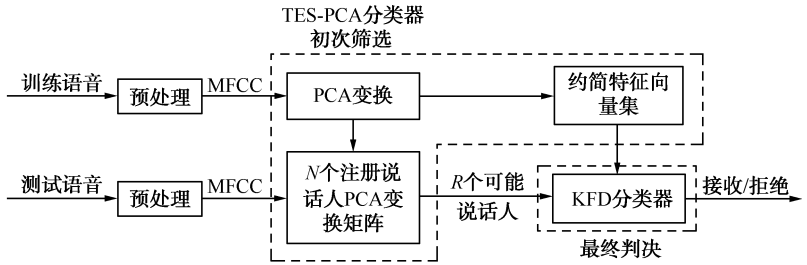


图 11.13　一种多级说话人确认方法系统框图

1）TES-PCA 初次筛选

注册说话人的 TES-PCA 分类器模型由两部分组成：一部分是通过降维得到的低维特征向量，另一部分是截断误差空间矩阵。

对每一位注册说话人的语音特征向量进行 PCA 分析变换之后，选择的前 q 个特征向量构成主成分空间 $\boldsymbol{P}^{(s)}=\{\boldsymbol{\mu}_1^{(s)},\boldsymbol{\mu}_2^{(s)},\cdots,\boldsymbol{\mu}_q^{(s)}\},s=1,\cdots,N$，相应地未选择的剩余特征向量构成截断误

差空间（Truncation Error Space，TES）$\boldsymbol{Q}^{(s)}=\{\boldsymbol{\mu}_{q+1}^{(s)},\boldsymbol{\mu}_{q+2}^{(s)},\cdots,\boldsymbol{\mu}_{q+m}^{(s)}\},s=1,\cdots,N$。将输入语音特征向量映射到 TES 得到该样本的截断误差：

$$\mathrm{TE}^{(s)}(\boldsymbol{x})=\left\|\boldsymbol{Q}^{(s)\mathrm{T}}(\boldsymbol{x}-\boldsymbol{m}_s)\right\|^2,s=1,\cdots,N \tag{11.28}$$

其中，$\boldsymbol{m}_s=\frac{1}{l}\sum_{t=1}^{l}\boldsymbol{x}_t^{(s)}$ 表示第 s 位说话人特征向量的均值向量。根据 PCA 变换的定义，输入说话人样本越接近目标说话人，其在 TES 映射得到的截断误差越小。因此，将输入样本映射到每一位说话人的 TES 计算截断误差，将计算出来的截断误差由小到大进行排序 $\mathrm{TE}^1(\boldsymbol{x})<\mathrm{TE}^2(\boldsymbol{x})<\cdots<\mathrm{TE}^N(\boldsymbol{x})$，选择前面最小的 R 个截断误差所对应的说话人作为 PCA 分类器的一级筛选结果。

2）核 Fisher 判别分类器

核 Fisher 判别技术是基于 Fisher 线性判别提出的一种二元分类方法，其核心思想是通过核函数将样本向量映射到一个高维空间，在此空间使用 Fisher 线性判别进行分类。该方法在模式识别领域具有良好的推广能力。

3）Fisher 线性判别

Fisher 线性判别[35]是一种应用极为广泛的两类分类技术，它根据最大化类间离散度、最小化类内离散度的准则，确定原始向量的投影方向，使各类之间最大程度地分离，从而达到正确的分类，如图 11.14 所示。样本集 1 和样本集 2 的数据的投影无论是在 x_1 轴或是在 x_2 轴上都是混杂的，因此单纯取它们在 x_1 或 x_2 上的投影都不能达到很好的分类效果。但是，在投影方向 w 上，两类样本很容易分开。

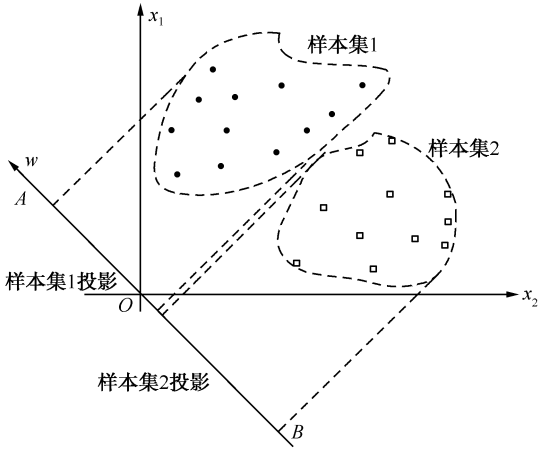


图 11.14　Fisher 线性判别示意图

设 $\boldsymbol{X}_1=\{\boldsymbol{x}_1^1,\cdots,\boldsymbol{x}_{C_1}^1\}$ 和 $\boldsymbol{X}_2=\{\boldsymbol{x}_1^2,\cdots,\boldsymbol{x}_{C_2}^2\}$ 是两类样本，$\boldsymbol{X}=\boldsymbol{X}_1\bigcup\boldsymbol{X}_2=\{\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_N\}$，

$C_1 + C_2 = N$，最佳投影方向可通过最大化下面目标函数求得：

$$J(\boldsymbol{w}) = \frac{\boldsymbol{w}^{\mathrm{T}} \boldsymbol{S}_b \boldsymbol{w}}{\boldsymbol{w}^{\mathrm{T}} \boldsymbol{S}_w \boldsymbol{w}} \tag{11.29}$$

其中，$\boldsymbol{w}$ 为投影方向；$\boldsymbol{S}_b$ 为类间离散度矩阵；$\boldsymbol{S}_w$ 为类内离散度矩阵，分别定义如下：

$$\boldsymbol{S}_b = (\boldsymbol{m}_1 - \boldsymbol{m}_2)(\boldsymbol{m}_1 - \boldsymbol{m}_2)^{\mathrm{T}} \tag{11.30}$$

$$\boldsymbol{S}_w = \sum_{i=1}^{2} \sum_{\boldsymbol{x} \in \boldsymbol{X}} (\boldsymbol{x} - \boldsymbol{m}_i)(\boldsymbol{x} - \boldsymbol{m}_i)^{\mathrm{T}} \tag{11.31}$$

其中，$\boldsymbol{m}_i (i = 1,2)$ 是各类样本的均值向量，

$$\boldsymbol{m}_i = \frac{1}{C_i} \sum_{j=1}^{C_i} \boldsymbol{x}_j^i \qquad (i = 1,2) \tag{11.32}$$

其中，$\boldsymbol{x}_j^i$ 表示第 $\boldsymbol{i}$ 类的第 j 个样本。最大化式（11.29）可得：

$$\boldsymbol{w} = \boldsymbol{S}_w (\boldsymbol{m}_1 - \boldsymbol{m}_2) \tag{11.33}$$

Fisher 线性判别解决问题的关键就是寻找一个最优的映射方向，而对于语音数据来说，数据分布呈非线性，线性判别显得过于简单，并不能达到好的分类性能。因此，在本文的说话人确认系统中提出使用基于核函数的 Fisher 判别进行分类。

2．核 Fisher 判别最终分类

核 Fisher 判别（KFD）的核心思想是，通过一个非线性映射 $\boldsymbol{\Phi}$ 将原始特征空间映射到一个新的特征空间 H，在新的特征空间 H 中使用 Fisher 线性判别进行分类，如图 11.15 所示。KFD 是 Fisher 线性判别的非线性扩展，可以很好地对非线性数据进行分类。

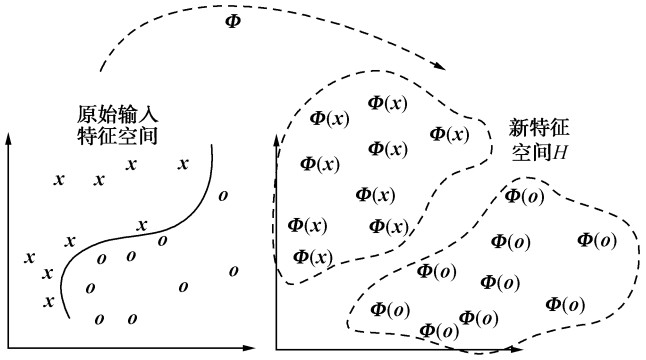


图 11.15　核 Fisher 判别特征映射 $\boldsymbol{\Phi}$ 示意图

在说话人确认中，每个说话人都有一个基于 Fisher 准则的最优映射方向，在这个映射方向上，目标说话人和其他说话人可以正确地区分开。将由 TES-PCA 得到的 R 个说话人语音向量作为核 Fisher 的输入，$\boldsymbol{X}_1=\{$目标说话人样本$\}$，样本数为 C_1，$\boldsymbol{X}_2=\{$其他说话人样本$\}$，样本数为 C_2，$C_1+C_2=N$。

在新的特征空间 H 中目标函数相应变为：

$$J(\boldsymbol{w})=\frac{\boldsymbol{w}^{\mathrm{T}}\boldsymbol{S}_b^{\Phi}\boldsymbol{w}}{\boldsymbol{w}^{\mathrm{T}}\boldsymbol{S}_w^{\Phi}\boldsymbol{w}} \tag{11.34}$$

其中，$\boldsymbol{S}_b^{\Phi}$ 和 $\boldsymbol{S}_w^{\Phi}$ 是相应的在 H 空间中的类间离散度矩阵和类内离散度矩阵；$\boldsymbol{w}$ 是投影方向。

$$\boldsymbol{S}_b^{\Phi}=(\boldsymbol{m}_1^{\Phi}-\boldsymbol{m}_2^{\Phi})(\boldsymbol{m}_1^{\Phi}-\boldsymbol{m}_2^{\Phi})^{\mathrm{T}} \tag{11.35}$$

$$\boldsymbol{S}_w^{\Phi}=\sum_{i=1}^{2}\sum_{\boldsymbol{x}\in\boldsymbol{X}}(\boldsymbol{\Phi}(\boldsymbol{x})-\boldsymbol{m}_i^{\Phi})(\boldsymbol{\Phi}(\boldsymbol{x})-\boldsymbol{m}_i^{\Phi})^{\mathrm{T}} \tag{11.36}$$

$$\boldsymbol{m}_i^{\Phi}=\frac{1}{C_i}\sum_{j=1}^{C_i}\boldsymbol{\Phi}(\boldsymbol{x}_j^i)\qquad i=1,2 \tag{11.37}$$

由于空间 H 的维数很高甚至是无穷维，直接求解是不可能的，可通过核函数的技巧，而不涉及具体的非线性运算。根据核函数理论，任何一个目标函数的解 $\boldsymbol{w}$ 都可以用特征空间中元素的线性组合表示：

$$\boldsymbol{w}=\sum_{i=1}^{N}a_i\boldsymbol{\Phi}(\boldsymbol{x}_i) \tag{11.38}$$

将式（11.38）和式（11.37）相乘并用核函数 $k(\boldsymbol{x}_j,\boldsymbol{x}_k^i)$ 代替相应的点积运算 $<\boldsymbol{\Phi}(\boldsymbol{x}_j),\boldsymbol{\Phi}(\boldsymbol{x}_k^i)>$ 得：

$$\boldsymbol{w}^{\mathrm{T}}\boldsymbol{m}_i^{\Phi}=\frac{1}{C_i}\sum_{j=1}^{N}\sum_{k=1}^{C_i}a_jk(\boldsymbol{x}_j,\boldsymbol{x}_k^i)=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{\mu}_i \tag{11.39}$$

这里，$\boldsymbol{\mu}_i=\frac{1}{C_i}\sum_{k=1}^{C_i}k(\boldsymbol{x}_j,\boldsymbol{x}_k^i)$，根据式（11.35）和式（11.39），可得：

$$\boldsymbol{w}^{\mathrm{T}}\boldsymbol{S}_b^{\Phi}\boldsymbol{w}=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{M}\boldsymbol{a} \tag{11.40}$$

$$\boldsymbol{w}^{\mathrm{T}}\boldsymbol{S}_w^{\Phi}\boldsymbol{w}=\boldsymbol{a}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{a} \tag{11.41}$$

其中，$\boldsymbol{M}=(\boldsymbol{\mu}_1-\boldsymbol{\mu}_2)(\boldsymbol{\mu}_1-\boldsymbol{\mu}_2)^{\mathrm{T}}$，$\boldsymbol{P}=\boldsymbol{P}_1+\boldsymbol{P}_2$，$\boldsymbol{P}_i=\boldsymbol{K}_i\boldsymbol{K}_i^{\mathrm{T}}-C_i(\boldsymbol{\mu}_i\boldsymbol{\mu}_i^{\mathrm{T}}),i=1,2$；$\boldsymbol{K}_i$ 为核函数矩阵，

$(\boldsymbol{K}_i)_{jk}=k(\boldsymbol{x}_j,\boldsymbol{x}_k^i)$ 其中 $i=1,2$， $j=1,2,\cdots,N$， $k=1,2,\cdots,N$； $\boldsymbol{x}_k^i$ 表示第 i 类第 k 个样本点。则式（11.34）可变为：

$$J(\boldsymbol{a})=\frac{\boldsymbol{a}^{\mathrm{T}}\boldsymbol{M}\boldsymbol{a}}{\boldsymbol{a}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{a}} \tag{11.42}$$

根据广义 Rayleigh 熵并忽略比例因子得 $\boldsymbol{a}=\boldsymbol{P}^{-1}(\boldsymbol{\mu}_1-\boldsymbol{\mu}_2)$，特征空间 H 中任一向量 $\boldsymbol{\Phi}(\boldsymbol{x})$ 在 Fisher 判定最优方向上的投影为：

$$\boldsymbol{w}\boldsymbol{\Phi}(\boldsymbol{x})=\sum_{i=1}^{N}a_i\boldsymbol{k}(\boldsymbol{x}_i,\boldsymbol{x}) \tag{11.43}$$

选择合适的阈值可得在新特征空间 H 中的分类判别函数为：

$$f(\boldsymbol{x})=\mathrm{sgn}[\boldsymbol{w}^{\mathrm{T}}\boldsymbol{\Phi}(\boldsymbol{x})+b]=\mathrm{sgn}[\sum_{i=1}^{N}a_i k(\boldsymbol{x}_i,\boldsymbol{x})+b] \tag{11.44}$$

目标说话人的训练语音特征参数根据 Fisher 准则得到最优映射方向，其测试语音特征参数通过式（11.43）计算出投影，最后使用分类判别函数式（11.44）即可得出识别结果。

11.6 小结

常用的说话人特征参数主要有 MFCC 系数和 LPCC 系数，识别方法主要有模板匹配法（VQ）、概率统计方法（HMM 模型，GMM 模型），辨别分类器的实现方法主要有人工神经网络和支持向量机等。说话人识别系统的研究和开发已经取得了较好的效果，在一些领域中得到了很好的应用。然而，目前无论是何种方法都还不能达到理想的识别效果，这不仅与语音信号本身易受噪声影响有关，而且也与所使用的分类技术的局限性有关。

为了进一步提升说话人识别系统的性能，需要在说话人特征提取、现有说话人模型的改进、新模型及识别策略等方面继续进行深入的研究。可概括为如下几个方面。

（1）寻找更好的语音处理方法，提取稳定且最富个性表现力的特征参数。

（2）针对说话人的语音特征随着年龄、情绪和健康状况等因素而变化的问题，寻找更具鲁棒性的特征参数。

（3）如何抽取特征样本，合理地选择样本数目，进而对样本进行建模。

（4）如何克服麦克风和信道对识别性能的影响。

（5）如何对真实声音和模仿声音进行准确的判别。

参 考 文 献

[1] 叶寒生．噪声环境下说话人识别方法研究．中国科学技术大学硕士学位论文，2008．

[2] S. Pruzansky , M.V. Mathews. Talker recognition procedure based on analysis of variance. Acoustical Society of America, 1964, 36(11)：2041-2047．

[3] S. Furui. Cepstral analysis technique for automatic speaker verification. IEEE Trans. Acoustics, Speech and Signal Processing, 1981,29(2)：254-272．

[4] F.K. Soong, A.E. Rosenberg, L.R. Rabiner, B.H. Zhuang. A Vector Quantization Approach to Speaker Recognition. In Proc. ICASSP, 1985：387-390．

[5] A.B. Poritz. Linear predictive hidden Markov models and the speech signal. Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, 1982：1291-1294．

[6] D.A. Reynolds, R.C. Rose. Robust Text-Independent Speaker Identification Using Gaussian Mixture Speaker Models. IEEE Transactions on Speech and Audio Processing,1995, 3(1)：72-83．

[7] C.N. Gedo, J.C. Eremic. Automatic Speaker Recognition System using the Discrete Hartley transform and an Artificial Neural Network. 1991 Conference Record of the Twenty-Fifth Asilomar Conference on Signals, Systems and Computers, 1991：1151-1154．

[8] J. Oglesby, J.S. Mason. Radial basis function networks for speaker recognition. In Proc. ICASSP, 1991：393-396．

[9] H. Gish, M. Schmidt. Text-independent speaker identification. IEEE Signal Processing Magazine, 1994, 11(4)：18-32．

[10] A. Erell, M. Weintraub. Filter-bank-energy estimation using mixture and Markov models recognition of noisy speech. IEEE Transactions on Speech and Audio Processing,1993，1(1)：68-76．

[11] 李明，张 勇，李军权，张亚芬．基于改进 PSO-SVM 的说话人识别方法．电子科技大学学报，2007，36(6)：1345-1349．

[12] 杨礼特．说话人识别系统研究与实现．西安电子科技大学硕士学位论文，2006．

[13] 张荣强．说话人识别中特征提取的方法研究．大连理工大学硕士学位论文，2005．

[14] W.M. Campbell，D.E. Sturim, D.A. Reynolds. Support vector machines using GMM supervectors for speaker verification. IEEE Signal Processing Letters, 2006, 13(5)：308-311．

[15] Ming Li，Yafen Zhang，Junquan Li，Yong Zhang. An Improved SVM Approach for

Speaker Identification. Journal of Computational Information Systems,2008,4(1)：1-6.

[16] W.M. Campbell, D.E. Sturim, D.A. Reynolds, A. Solomonoff. SVM Based Speaker Verification using a GMM Supervector Kernel and NAP Variability Compensation. In Proc. ICASSP,2006：97-100.

[17] J.R. Hershey, P.A. Olsen. Approximating the Kullback Leibler Divergence between Gaussian Mixture Models. In Proc. ICASSP , 2007：317-320.

[18] Ming Li, Xueyan Liu, Fuwen Wu .Speaker Identification based on Multi-Reduced SVM. The 3rd International Conference on Natural Computation (ICNC'07) and the 4th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD'07), 2007：371-375.

[19] 刘雪燕，李明．基于 PCA 和多约简 SVM 的多级说话人辨识. 计算机应用，2008，28(1)：127-130.

[20] Xiaolei Xia, Kang Li. Tree-Structured Learning of Multi-class SVMs with Triple Learning Units. Natural Computation, ICNC '09. Fifth International Conference , 2009：363 - 367.

[21] 钱博，李燕萍，唐振民，徐利敏. 基于神经网络集成的说话人识别算法仿真研究.系统仿真学报，2008,20(5)：1285-1288.

[22] 潘镭．基于混合高斯模型的说话人识别．中国科学技术大学硕士学位论文，2009.

[23] 付中华．说话人识别系统鲁棒性研究．西北工业大学博士学位论文，2004.

[24] Fenglei Hou, Bingxi Wang. Text-independent speaker recognition using support vector machines. In Proceeding of ICII,2001：402-407.

[25] Y.J. Lee, O.L. Mangasarian. RSVM：Reduced support vector machine. In Proceeding of the First SIAM International Conference on Data Mining, 2001：350-366.

[26] Songfeng Zheng, Xiaofeng Lu, Nanning Zheng et al. Unsupervised clustering based reduced support vector machines. The Institute of Artificial Intelligence and Robotics, ICASSP 2003：821-824.

[27] Fangfang Wu, Yinliang Zhao. A novel Multi-reduced Support Vector Machine. ICNN & B’2005 International Conference,2005：322-326.

[28] SY Sun, CL Tseng, YH Chen, et al. Cluster-based support vector machines in text-independent speaker identification. 2004 IEEE International Joint Conference on Neural Networks, 2004：729-734.

[29] B Sun, W Liu, Q Zhong. Hierarchical speaker identification using speaker clustering. In Proc. International Conference on Natural Language Processing and Knowledge Engineering,2003：299-304.

[30] Wei-Ho Tsai, Shih-Sian Cheng, Hsin-Min Wang. Automatic Speaker Clustering Using a Voice Characteristic Reference Space and Maximum Purity Estimation. IEEE Transition on andio, and language processing,2007,15(4)：1461-1471.

[31] S. Mika, G. ROatsch, J. Weston, B. SchOolkopf, K.R. MOuller. Fisher discriminant analysis with kernels. IEEE Neural Networks for Signal Processing IX,1999：41-48.

[32] 肖建华．智能模式识别方法．广州：华南理工大学出版社，2006.

[33] Ming Li, Yu-Juan Xing, Rui-Ling Luo. A Novel Feature Extraction Based on PCA and Improved Fisher score applied in Speaker verification. 2008 International Conference on Audio, Language and Image Processing, 2008：56-60.

[34] Junwen Wu, Xuegong Zhang. A PCA Classifier and Its Application in Vehicle Detection. IEEE International Joint Conference on Neural Networks, 2001：600-604.

[35] Shu Yang, Shuicheng Yan, Chao Zhang. Bilinear Analysis for Kernel Selection and Nonlinear Feature Extraction. IEEE Transactions on Neural Networks,2007, 18(5)：1442-1452.

反侵权盗版声明

《智能信息处理与应用》读者意见反馈表

尊敬的读者：

感谢您惠购本书。为了能为您提供更优秀的教材，请您抽出宝贵的时间，将您的意见以下表的方式（可从 http://www.hxedu.com.cn 下载本调查表）及时告知我们，以改进我们的服务。对采用您的意见进行修订的教材，我们将在该书的前言中进行说明并赠送您样书。

姓名：_____ 电话：_____

职业：_____ E-mail：_____

邮编：_____ 通信地址：_____

1．您对本书的总体看法是：

□很满意 □比较满意 □尚可 □不太满意 □不满意

2．您对本书的结构（章节）：□满意 □不满意 改进意见_____

3. 您对本书的例题： □满意 □不满意 改进意见_____

4．您对本书的习题： □满意 □不满意 改进意见_____

5．您对本书的实训： □满意 □不满意 改进意见_____

6． 您对本书其他的改进意见：

7．您感兴趣或希望增加的教材选题是：

请寄：100036 北京市海淀区万寿路 173 信箱机电与交通分社 李洁 收

电话：010–88254501 E-mail：lijie@phei.com.cn